

Softex LLC v. Absolute Software Corporation et al., No. 1:22-cv-01308 (W.D. Tex.)
Infringement of U.S. Patent No. 8,506,649

This chart shows, on an element-by-element basis, how Absolute Software Corporation and Absolute Software, Inc. (collectively “Absolute”) infringe Claims 1, 7, 9, 15 of U.S. Patent No. 8,506,649 (the “’649 Patent”) through the making, using, offering for sale, or sale in the United States, and/or importation into the United States, of various products and offerings, including Absolute’s persistent theft detection software accused of infringing the Asserted Patents in Softex’s Complaint and/or in Softex’s Infringement Contentions. They include, but are not limited to, Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, Absolute Visibility, Absolute Control, Absolute Resilience, and Computrace software (collectively referred to as “Accused Instrumentalities”), as well as any other products that Absolute makes, uses, offers for sale, or sells in the United States, and/or imports into the United States that operate in the manner set forth below.

Softex LLC (“Softex”) further states that Absolute also indirectly infringes each asserted claim in violation of 35 U.S.C. § 271(b) by taking active steps to encourage and facilitate direct infringement by third parties in the United States, including customers, partners, and service providers, through the dissemination of the Accused Instrumentalities and the creation and dissemination of promotional and marketing materials, supporting materials, instructions, product manuals, and/or technical information relating to such products with knowledge and the specific intent that its efforts would result in the direct infringement of the ’649 Patent. For example, Absolute took active steps to encourage service providers and other customers to use the Accused Instrumentalities in the United States in a manner that would directly infringe each element as described below, including by marketing the functionality and creating and distributing

various training programs for use of it. Non-limiting examples of such actions include the following: “Absolute Partners with leading organizations to bring Endpoint Resilience across the globe.” (<https://www.absolute.com/partners/our-partners/>); “We've built strong relationships with manufacturers around the world so that today, most devices roll off the assembly line with Persistence from Absolute already embedded in the firmware of the machine. Click any of the logos below to see specific devices that Absolute is embedded in.” (<https://www.absolute.com/partners/device-manufacturers/>); “To activate a persistent, unbreakable connection to your devices, you'll need to install a small, client-side agent.” “First, install the agent on a single device to test your installation: 1. Confirm connectivity with the Network Diagnostics Tool 2. Download the Absolute Agent and install it on your first device 3. Confirm device activation by checking the Assets page Success! Now you can enroll your remaining devices.” (<https://go.absolute.com/Onboarding-Enroll-devices-Step2.html>); “Absolute may be downloaded, installed, and then verified by following these instructions.” (“<https://www.dell.com/support/kbdoc/en-us/000131897/how-to-download-and-install-absolute>”); “You can activate your Absolute Home & Office subscription in just three easy steps” “Purchase a 1-, 2-, or 3-year Absolute Home & Office subscription” “Check your inbox Look for a welcome email containing your subscription’s activation code” “Download, install, and activate Follow the email instructions to activate Absolute Home & Office on your PC, tablet or smartphone. That’s it!” (<https://www.hp.com/us-en/services/consumer/theft-protection.html>); “Click: ACTIVATE ACCOUNT ... “A unique installer is generated. This process typically takes about three minutes. Once generated, click on INSTALL APPLICATION” ... “New users are prompted to create an account password. Existing users are prompted to sign in. After signing in, the Lenovo Smart Lock portal (<https://lenovosignin.absolute.com>) appears.” (<https://support.lenovo.com/us/en/solutions/ht512830-lenovo-smart-lock-services-locate-lock-and-recover-your-pc-anytime->

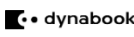
anywhere”); *see also* (<https://www.lenovo.com/us/en/d/accessories/absolute/?orgRef=https%253A%252F%252Fwww.google.com%252F>), as well as the materials cited below. Absolute thus induced, and continues to actively induce, the direct infringement of the ’629 Patent by service providers and other customers by distributing the Accused Products and, among other things, creating and distributing various programs that train customers to use them in an infringing manner.

Softex further notes that this chart contains an exemplary, non-limiting description of Absolute’s infringement that is representative of how each Accused Instrumentality infringes the ’649 Patent. Softex further notes that it makes these contentions based on the information reasonably available to it at this time because discovery has not commenced, and Absolute has not provided any documents concerning its infringement, including any source code for the Accused Instrumentalities.

As demonstrated below, Softex contends that each element of each asserted claim is literally infringed by the Accused Instrumentalities. Softex further contends that, to the extent that any particular element is shown not to be met literally by the Accused Instrumentalities, each Accused Instrumentality infringes under the doctrine of equivalents for the reasons set forth below because there would be no substantial difference between the elements of the asserted claims and the corresponding functionality in the Accused Instrumentality, i.e., the corresponding functionality in the Accused Instrumentality does substantially the same thing, in substantially the same way, to achieve substantially the same result(s) as the claimed elements.

Further, the Court has yet to issue its claim construction rulings. Softex thus reserves its right to modify, supplement, and/or amend these contentions as additional evidence and information become available, including in light of discovery, invalidity, prior art, claim construction, or any information provided by Absolute or any other party or non-party to this action.

Electronic device security and tracking system and method
U.S. Patent No. 8,506,649

Claims	
[1pre] A mobile electronic device, comprising:	The Accused Instrumentalities comprise “a mobile device, comprising.” Absolute Home & Office is installed on laptops comprising mobile electronic devices. BIOS & Firmware Compatibility Checker Are your endpoints compatible? Probably — <u>Absolute Persistence</u> is <u>already embedded in devices</u> made by the world’s leading manufacturers before they leave the factory. But if you need more clarity, choose a manufacturer below to see which models are supported.                     https://www.absolute.com/partners/device-compatibility/ For example, Absolute Persistence is preinstalled on the following Dell notebooks and tablets:

	Notebooks & Tablets Models
	Alienware Area-51M R2, Aurora R11, Aurora R12, Aurora R13, Aurora Ryzen, Aurora Ryzen R14, M11x, M15x, M17x, M18x, X15x, X17x

	Inspiron	1010, 1011, 1012, 1018, 1090, 1110, 1120, 1121, 1122, 11z, 1200, 1210, 13, 1300, 130B, 1318, 13z, 14 N4050, 1420, 1440, 1464, 1470, 14R, 14z Ultrabook, 15, 1501, 1520, 1521, 1525, 1526, 1545, 1546, 1564, 1570, 15R, 15z Ultrabook, 17, 1720, 1721, 1745, 1750, 1764, 17R, 2200, 3000 2n1, 3000 Series, 3050, 3052, 3059, 3060, 3064, 3135, 3137, 3147, 3152, 3153, 3157, 3158, 3162, 3163, 3164, 3168, 3169, 3179, 3180, 3185, 3195 2n1, 3250, 3252, 3263, 3265, 3268, 3275, 3277, 3290 AIO, 3420, 3421, 3437, 3441, 3442, 3443, 3451, 3452, 3455, 3458, 3459, 3462, 3464 AIO, 3465, 3467, 3468, 3470, 3475, 3475 AIO, 3477 AIO, 3480 AIO, 3481, 3482, 3490, 3493, 3501, 3502, 3505, 3510, 3511, 3515, 3520, 3521, 3531, 3537, 3541, 3542, 3543, 3551, 3552, 3555, 3558, 3559, 3565, 3567, 3568, 3573, 3576, 3580, 3581, 3582, 3583, 3584, 3585, 3590, 3593, 3595, 3650, 3655, 3656, 3668, 3670, 3721, 3737, 3790, 3793, 3880, 3881, 3891, 5000 2n1, 5000 Series, 5310, 5323, 5348, 5368, 5370, 5378, 5379, 5390, 5391, 5400 2n1, 5401, 5410, 5410 2n1, 5420, 5421, 5423, 5425, 5435, 5437, 5442, 5447, 5448, 5451, 5452, 5455, 5457, 5458, 5459, 5468, 5481 2n1, 5480, 5482, 5485, 5490, 5490 2n1, 5491 2n1, 5493, 5494, 5498, 5501, 5510, 5515, 5518, 5520, 5521, 5523, 5525, 5535, 5537, 5542, 5543, 5545, 5547, 5548, 55755551, 5552, 5555, 5557, 5558, 5559, 5565, 5566, 5567, 5568, 5570, 5576, 5577, 5578, 5579, 5580, 5582, 5584, 5585, 5583, 5584, 5590, 5591 2n1, 5593, 5594, 5598, 5720, 5721, 5735, 5737, 5748, 5749, 5755, 5758, 5759, 5765, 5767, 5770, 6000, 630, 6400, 640M, 7000 Series, 700M, 710M, 7300 2n1, 7348, 7352, 7353, 7359, 7368, 7370, 7373, 7375, 7378, 7380, 7386, 7390 2n1, 7391, 7391 2n1, 7405 2n1, 7415, 7420, 7437, 7459, 7447, 7460, 7466, 7467, 7472, 7490, 7500 2n1, 7501, 7520, 7537, 7547, 7548, 7557, 7558, 7559, 7560, 7566, 7567, 7568, 7569, 7570, 7572, 7573, 7577, 7579, 7580, 7586, 7599, 7590, 7590 2n1, 7591, 7591 2n1, 7610, 7700 AIO, 7720, 7737, 7746, 7773, 7775, 7778, 7779, 7786, 7790 AIO, 7791 2n1, 9300, 9400, B120, B130, Duo Tablet, E1405, E1505, E1705, M101z, M102z 1122, M301Z, M4010, M4040, M4110, M5010, M5030, M5040, M5110, N3010, N301Z, N311Z
--	----------	--

	Latitude	10 Tablet, 110L, 12 Tablet Extreme 7214, 12 Tablet Rugged 7202, 120L, 13, 131L, 14 Rugged, 14 Rugged Extreme, 2100, 2110, 2120, 3120, 3150, 3160, 3180, 3189, 3190, 3190 2-In-1, 3300, 3301, 3310, 3310 2-in-1, 3311, 3320, 3330, 3340, 3350, 3379, 3380, 3390 2-In-1, 3400, 3410, 3420, 3440, 3450, 3460, 3470, 3480, 3490, 3500, 3510, 3520, 3540, 3550, 3560, 3570, 3580, 3590, 4310, 5175, 5179, 5250, 5280, 5285, 5289, 5290, 5290 2-In-1, 4300, 5300, 5300 2-in-1, 5310, 5310 2-in-1, 5320, 5330, 5400, 5401, 5404, 5410, 5411, 5414, 5420, 5421, 5424, 5430, 5431, 5450, 5480, 5480, 5488, 5490, 5491, 5495, 5500, 5501, 5510, 5511, 5520, 5521, 5530, 5531, 5550, 5580, 5580, 5590, 5591, 6410, 6410 ATG, 6430u, 6510, 7200 2-in-1, 7210 2n1, 7212, 7214, 7220, 7250, 7275, 7280, 7285, 7290, 7300, 7310, 7320, 7320 Detachable Gen 12, 7330, 7350, 7370, 7380, 7389, 7389 2-in-1, 7390, 7390 2-In-1, 7400, 7400 2-in-1, 7404, 7410, 7414, 7420, 7424 7430, 7450, 7480, 7490, 7520, 7530, 9330, 9410, 9410 2n1, 9420, 9430, 9510, 9520, D410, D420, D430, D510, D520, D530, D531, D610, D620, D630, D630 XFR, D631, D810, D820, D830, E4200, E4300, E4310, E5000, E5250, E5270, E5400, E5410, E5414, E5420, E5430, E5440, E5450, E5460, E5470, E5470, E5500, E5510, E5520, E5520M, E5530, E5540, E5550, E5570, E6000, E6220, E6230, E6320, E6330, E6400, E6400 ATG, E6400 XFR, E6410, E6410 ATG, E6420, E6420 ATG, E6430, E6430 ATG, E6430S, E6430S, E6430u, E6440, E6500, E6510, E6520, E6530, E6540, E7214, E7240, E7250, E7270, E7414, E7440, E7450, E7470, ST Tablet, X1, XT, XT2, XT2 XFR, XT3 Tablet, Z, Z600
	Latitude Rugged	5414 Rugged, 5420 Rugged, 5424 Rugged, 5430 Rugged, 7202 Rugged Tablet, 7204 Rugged Extreme, 7212 Rugged Extreme Tablet, 7214 Rugged Extreme Tablet, Latitude 7220 Rugged Extreme Tablet, 7330 Rugged, 7414 Rugged Extreme, 7424 Rugged Extreme
	Netbook UMPC	Inspiron Duo Convertible, Inspiron Mini 10, Inspiron Mini 1010, Inspiron Mini 1011, Inspiron Mini 1012, Inspiron Mini 1018, Inspiron Mini 12, Inspiron Mini 9, Inspiron Mini 910, Latitude 2100, Latitude 2120

	Precision	3510, 3520, 3530, 3540, 3550, 3541, 3551, 3560, 3561, 3571, 3620, 3630, 3650, 390, 3930, 490, 5510, 5520, 5530, 5530 2-In-1, 5540, 5550, 5560, 5720 All-In-One, 5750, 5760, 690, 5810, 5820, 7510, 7520, 7530, 7540, 7550, 7560, 7710, 7720, 7730, 7740, 7750, 7760, 7810, 7820, 7920, M20, M2300, M2400, M2800, M3800, M4300, M4400, M4500, M4600, M4700, M4800, M5520, M5530, M6300, M6400, M65, M6500, M6600, M6700, M6800, M70, M90
	Studio	15, 16, 17
	Venue Tablets	Venue 10 Pro Tablet, Venue 11 Pro Tablet, Venue 8 Pro Tablet
	Vostro	1000, 1014, 1015, 1088, 1200, 1220, 1310, 1320, 1400, 1440, 1450, 1500, 1510, 1520, 1540, 1550, 1700, 1710, 1720, 2420, 2421, 2520, 2521, 3070, 3250, 3267, 3268, 3300, 3350, 3360, 3400, 3401, 3405, 3420, 3445, 3446, 3449, 3450, 3458, 3459, 3460, 3468, 3470, 3471, 3478, 3480, 3481, 3490, 3491, 3500, 3501, 3510, 3511, 3515, 3546, 3549, 3550, 3555, 3558, 3559, 3560, 3561, 3562, 3565, 3568, 3578, 3580, 3581, 3583, 3590, 3591, 3650, 3650, 3653, 3660, 3667, 3668, 3669, 3670, 3671, 3681, 3700, 3750, 3888, 5090, 5310, 5390, 5391, 5401, 5402, 5410, 5459, 5460, 5468, 5470, 5471, 5480, 5481, 5490, 5501, 5510, 5560, 5568, 5581, 5590, 5880, 7500, 7510, 7570, 7580, 7590, A840, A860, A90, V130, V131
	XPS	11 Ultrabook, 12 Ultrabook, 13 Ultrabook, 14 Ultrabook, 14z, 15, 15z, 720, M1210, M1330, M140, M1530, M170, M1710, M1730, M2010, XPS 12, XPS 13, XPS 15, XPS 17, XPS 17 3D, XPS 18, 12 9Q23, 12-9Q33, 13 7300, 13 7390, 13 7390 2-in-1, 13 9300, 13 9305, 13 9310, 13 9310 2-in-1, 13 9343, 13 9350, 13 9360, 13 9365, 13 9370, 13 9380, 15 7590, 15 9500, 15 9510, 15 9530, 15 9550, 15 9560, 15 9570, 15 9575, 17 9700, 17 9710,
	https://www.absolute.com/partners/device-compatibility/#dell For example, Absolute Persistence is preinstalled on the following HP notebooks and tablets:	

	Notebooks & Tablets	Models
	Compaq nc Series Notebook	2400, 4200, 4400, 6120, 6220, 6230, 6320, 6340, 6400, 8230, 8240, 8430
	Compaq nw Series Mobile Workstation	8240, 8440, 9440
	Compaq nx Series Notebook	6110, 6120, 6310, 6315, 6320, 6325, 6330, 7300, 7400, 9420
	Compaq Presario Series	A900, B1200, C7, C700, CQ20, CQ32, CQ35, CQ36, CQ40, CQ41, CQ42, CQ43, CQ45, CQ50, CQ56, CQ57, CQ58, CQ60, CQ60Z, CQ61, CQ62, CQ70, CQ71, CQ72, F7, F700, V3500, V3600, V3700, V6, V6500, V6700
	Envy Series	All Models
	HDX Series	16t, 18t
	HP Compaq 2000 Series Notebooks	2133, 2210b, 2230s, 2510p, 2710p
	HP Compaq 6000 Series Notebooks	6440b, 6445b, 6510b, 6515b, 6520s, 6530b, 6530s, 6535b, 6535s, 6540b, 6710b, 6710s, 6715b, 6715s, 6720s, 6730b, 6730s, 6735b, 6735s, 6820s, 6830s, 6910p, 6930p
	HP Compaq 8000 Series	8510p, 8510w, 8710p, 8710w, 8740w
	HP Compaq Tablet PC	TC4200, TC4400

	HP Elite Series (EliteBook and ElitePad)	2170p, 2530p, 2540p, 2560p, 2570p, 2730p, 2740p, 2760p, 2770m, 360 G3, 405 G8, 640 G9, 645 G9, 650 G9, 6540b, 6930p, 720 G1, 720 G2, 725 G2, 725 G3, 725 G4, 735 G5, 735 G6, 740G1, 740G2, 745 G2, 745 G3, 745 G4, 745 G5, 745 G6, 750 G1, 750 G2, 755 G2, 755 G3, 755 G4, 755 G5, 800 G3, 820 G1, 820 G2, 820 G3, 820 G4, 830 G5, 830 G6, 830 G7, 830 G8, 830 G9, 835 G7, 835 G8, 840 G1, 840 G2, 840 G3, 840 G4, 840R G4, 840 G5, 840 G5 HC, 840 G6, 840 G6 HC, 840 G7, 840 G8, 840 G9, 840r G4, 8440p, 845 G7, 845 G8, 846, 846 G5, 8460p, 8460w, 8470p, 8470w, 850 G1, 850 G2, 850 G3, 850 G4, 850 G5, 850 G6, 850 G7, 850 G8, 8530p, 8530w, 8540p, 8540w, 855 G7, 855 G8, 856, 860 G9, 8560p, 8560w, 8570p, 8570w, 8730w, 8740w, 876, 8760w, 8770w, 940 G1, Elite x2 1011 G1, Elite X2 1012 G1, ElitePad 1000 G2, ElitePad 1000 G2 Rugged Tablet, ElitePad 1040 G1, ElitePad 900, Folio 1020, Folio 1040 G3, Folio 1040 G4, Folio 1040 G5, 1040 G7, HP Elitebook 755 G3, HP EliteBook 850 G3, Revolve 210 G2, Revolve 810 G1, Revolve 810 G2, Revolve 810 G3, x360 830 G7, x360 830 G8, x360 830 G9, 1030 G1, 1050 G1, x360 830 G5, x360 830 G6, x360 830 G7, x360 830 G8, x360 1020 G2, x360 1030 G1, x360 1030 G2, x360 1030 G3, x360 1030 G4, x360 1030 G7, x360 1030 G8, x360 1040 G9, x360 1040 G5, x360 1040 G6, x360 1040 G7, x360 1040 G8, Dragonfly, Dragonfly G2, Dragonfly Max, X2 G1, X2 G2, X2 G3, X2 G4, Elite X2 G8
	HP Folio Series (Ultrabook)	1020 G1, 1020 G2, 1020 G3, 1030 G1, 1040 G1, 1040 G2, 1040 G3, 1040 G4, 1040 G9, 1050 G1, 13, 940 G1, 9470M, 9480M
	HP Laptop	g4, G42, g6, G60, G61, G62, g7, G70, G71, G72, HP 2000, HP 430, HP 630, HP/Compaq 435, HP X360, HP X360 310 G1 PC, HP X360 310 G2 PC, Pro X2 410 G1, Pro X2 612 G1
	HP Notebook PC	210 G1, 215 G1, 240, 240 G2, 240 G3, 240 G4, 240 G5, 240 G6, 240 G7, 240 G8, 242, 245, 245 G2, 245 G3, 245 G4, 245 G5, 245 G6, 245 G7, 245 G8, 246 G7, 250, 250 G2, 250 G3, 250 G4, 250 G5, 250 G6, 250 G7, 250 G8, 255, 255 G2, 255 G3 255 G4, 255 G5, 255 G6, 255 G7, 255 G8, 3115m, 3125, 340 G1, 340 G2, 340S G7, 348 G4, 348 G5, 348 G7, 350 G1, 350 G2, 355 G2, 360 G3, 450, 455, 470 G7, 470 G8, 650, 655, 245 G6

	HP Pro Series	HP Pro Slate 10 EE, Pro Tablet 10 EE, Pro Tablet 610 G1
	HP Slate Tablet PC	HP Pro Slate 10 EE G1, HP Slate 2, HP Slate 500
	HP Spectre Series	13 Pro, 13 X2, Pro X360 G1, Pro X360 G2, X2 1011 G1, X360 Convertible, X360 2iO, XT Pro, XT Pro 13, XT Touchsmart, XT Ultrabook, 13 Ultrabook
	HP Stream	11, 11 PRO G3 NOTEBOOK PC, 13, 14, 14 Pro
	HP ZBook Mobile Workstation	14, 14 G2, 14 G8, 14 G9, 14U G4, 14U G5, 14U G6, 14U G7, 15, 15 G2, 15 G3, 15 G4, 15 G5, 15 G6, Create G7, Fury 15 G7, Fury 15 G8, Fury 16 G9, Fury 17 G7, Fury 17 G8, Fury 17 G9, 15U G2, 15U G3, 15U G4, 15U G5, 15U G6, 15V G5, 17, 17 G2, 17 G3, 17 G4, 17 G5, 17 G6, 17 G8, Power G7, Power G8, Studio G3, Studio G4, Studio G5, Studio X360 G5, Studio G6, Studio G7, Studio G8, Studio G9, ZB15G5, Firefly 14 G7, Firefly 14 G8, Firefly 15 G7, Firefly 15 G8
	Mini	1103, 1104, 2102, 2133, 2134, 2140, 3105M, 3115, 3125, 5101, 5102, 5103
	Omen & Victus (gaming)	15, 15T, 16, 16T, 16Z, 17, 17T
	Pavilion dm Series	dm1, dm3, dm4
	Pavilion dv Series	dv2, dv3, dv4, dv5, dv6, dv7, dv8, dv9, tx1, tx2
	Pavilion Laptop	13, 14, 14Z, 15, 15T, 15Z, Gaming 16
	Pavilion x360 Convertible	14, 14M, 15

ProBook

11 EE, 11 G1, 11 G2, 11 G5, 400 G4, 4230s, 430, 430 G2, 430 G3, 430 G4, 430 G5, 430 G6, 430 G7, 430 G8, 4310s, 4311s, 4320s, 4321s, 4325s, 4326s, 4330s, 4331s, 4340s, 4341s, 440 G1, 440 G2, 440 G3, 440 G4, 440 G5, 440 G6, 440 G7, 440 G8, 440 G9, 4410s, 4411s, 4415s, 4416s, 4420s, 4421s, 4425s, 443, 4430s, 4431s, 4435s, 4436s, 4440s, 4441s, 4445s, 4446s, 445 G1, 445 G2, 445 G6, 445 G7, 445 G8, 445 G9, 445R G6, 4470s, 4470s, 450 G1, 450 G2, 450 G3, 450 G4, 450 G5, 450 G6, 450 G7, 450 G8, 450 G9, 4510s, 4515s, 4520s, 4525s, 453, 4530s, 4535s, 4540s, 4545s, 455, 455 G1, 455 G2, 455 G3, 455 G4, 455 G5, 455 G6, 455 G7, 455 G8, 455 G9, 455R G6, 470, 470 G1, 470 G2, 470 G3, 470 G4, 470 G5, 4710s, 4720s, 4730s, 4740s, 5220m, 5310m, 5320m, 5330m, 600 G4, 600 G5, 6360b, 630 G8, 635 Aero G7, 635 Aero G8, 640 G1, 640 G2, 640 G3, 640 G4, 640 G5, 640 G8, 640 G9, 6440b, 6445b, 645 G1, 645 G2, 645 G4, 6450b, 6455b, 646, 6460b, 6465b, 6470b, 6475b, 650 G1, 650 G2, 650 G3, 650 G4, 650 G5, 650 G8, 6540b, 6545b, 655 G1, 655 G2, 6550b, 6555b, 6560b, 6565b, 6570b, x360 11 G2, x360 11 G3, x360 11 G4, x360 11 G5, x360 11 G6, x360 11 G7, x360 440 G1, x360 435 G7, x360 435 G8

<https://www.absolute.com/partners/device-compatibility/#hp>

For example, Absolute Persistence is preinstalled on the following Lenovo notebooks and tablets:

	Notebooks & Tablets	Models
	Essentials	B40-30, B40-45, B40-80, B430, B4450s, B480, B490, B50-45, B560, B580, B590, E49, G40-80, K49, K490s, M4400, M490, M490s, M495, V110, V310, V330, V340, V480, V490, V490u, V510, V510z, V580, V580c
	IdeaPad	100, 110, 300, 310, 310 TOUCH, 305, 320, 320 TOUCH, 320C, 330, 500, 510, 510S, 520, 720S, 3000, 3105, D330, Duet 3, FLEX 4, Flex 14, FLEX 15, MIIX 320, MIIX 520, MIIX 700, N580, N581, P580, P585, S10, S10e, S205S, S206, S300, S310, S400, S410, S400 Touch, S540, S9e, U160, U260, U300(s), U310, U310 Touch, U330P, U330 Touch, U430P, U430 Touch, U400, U410, U410 Touch, U430 Touch, U510, U530 Touch, V130, V330, Y400, Y410P, V460, Y480, Y510p, Y580, Y700, Yoga 11, Yoga 11S, Yoga 13, YOGA 2 PRO, Yoga 900, Yoga 910, Z410, Z460, Z465, Z510, Z560, Z565
	ThinkPad	10 1st GEN, 10 2ND GEN, 11E 1st GEN, 11E 2ND GEN, 11E 3RD GEN, 11E 4TH GEN, 11E 5TH GEN, 11E YOGA GEN 6, 13 1ST GEN, 13 2ND GEN, 13 3RD GEN, YOGA 370, ThinkPad 25
	ThinkPad A Series	A275, A285, A475, A485
	Thinkpad Edge Series / E Series	E13, E14, E14 GEN 2, E14 GEN 3, E14 GEN 4, E15, E15 GEN 2, E15 GEN 3, E10, E120, E125, E130, E135, E145, E220s, E30, E31, E320, E325, E330, E335, E40, E420, E420s, E425, E430, E430c, E431, E435, E440, E445, E450, E450c, E455, E460, E465, E470, E470c, E475, E480, E485, E49, E490, E490s, E495, E50, E520, E525, E530, E530(c), E531, E535, E540, E545, E550, E550c, E555, E560, E565, E570, E570c, E575, E580, E585, E590, E595, HELIX GEN 2, S230u, S430, Twist
	ThinkPad G Series	G460, G40, G470, G480, G50, G550, G560, G570, G580, G780
	ThinkPad L Series	L13 GEN 1, L13 GEN 2, L13 GEN 2A, L13 YOGA GEN1, L13 YOGA GEN 2, L14 GEN 1, L14 GEN 2, L14 GEN 2A, L14 GEN 3, L15 GEN 1, L15 GEN 2, L15 GEN 2A, L14 GEN 3, L330, L380, L380 Yoga, L390, L390 Yoga, L410, L411, L412, L420, L421, L430, L440, L450, L460, L470, L480, L490, L510, L512, L520, L530, L540, L560, L570, L580, L590

	ThinkPad P Series	P1, P1 GEN 2, P1 GEN 3, P1 GEN 4i, P14S GEN 1, P14S GEN 2, P15 GEN 1, P15S GEN 1, P15 GEN 2, P15S GEN 2, P15V GEN 1, P15V GEN 2, P17 GEN 1, P17 GEN 2, P40 YOGA
	ThinkPad Mobile Workstation	P1, P40, P43s, P50, P50s, P51, P51s, P52, P52s, P53, P53s, P70, P71, P72, P73, W500, W510, W520, W530, W540, W541, W550s, W700, W700ds, W701, W701ds
	ThinkPad R Series	R400, R480, R500, R51e, R52, R60, R60e, R61, R61e, R61i
	ThinkPad SL Series	SL300, SL400, SL400c, SL410, SL500, SL500c, SL510, SL512
	ThinkPad S Series	S1 YOGA, S1 YOGA 12, S1 YOGA GEN 2, S2, S3 YOGA 14, S430, S5, S5 YOGA 15
	ThinkPad T Series	T14 GEN 1, T14 GEN 2, T14S GEN 1, T15 GEN 1, T15 GEN 2, T15G GEN 1, T15G GEN 2, T15P GEN 1, T400, T400s, T410, T410i, T410s, T410si, T420, T420i, T420s, T420si, T43, T430, T430s, T430u, T431s, T43p, T440, T440p, T440s, T450, T450s, T460, T460p, T460s, T462, T470, T470p, T470s, T480, T480s, T490, T490s, T495, T495S, T500, T510, T510i, T520, T520i, T530, T540p, T550, T560, T560s, T570, T580, T590, T60, T60p, T61, T61p
	ThinkPad Tablet & Hybrid	Helix, Miix 310, Miix 320, Miix 510, Miix 700, Miix 720, Tablet 2, Tablet (Android), ThinkPad 10, ThinkPad 8, ThinkPad Yoga, ThinkPad Yoga 260, Thinkpad Yoga 370

ThinkPad X Series	X1, X1 Carbon, X1 Carbon GEN 2, X1 Carbon GEN 3, X1 Carbon GEN 4, X1 Carbon GEN 5, X1 Carbon GEN 6, X1 Carbon GEN 7, X1 Carbon GEN 8, X1 Carbon GEN 9, X1 Carbon GEN 10, X1 Carbon Touch, X1 Extreme GEN 1, X1 Extreme GEN 2, X1 Extreme GEN 3, X1 Extreme GEN 4, X1 FOLD GEN 1, X1 NANO GEN 1, X1 Tanium GEN 1, X1 Tablet GEN 1, X1 Tablet GEN 2, X1 Tablet GEN 3, X1 Yoga GEN 1, X1 Yoga GEN 2, X1 Yoga GEN 3, X1 Yoga GEN 4, X1 Yoga GEN 5, X1 Yoga GEN 6, X12 Detachable GEN 1, X13 GEN 1, X13 GEN 2, X13 YOGA GEN 1, X13 YOGA GEN 2, X13 YOGA GEN 3, X13S YOGA GEN 1, X100e, X120e, X121e, X130e, X131e, X140e, X141e, X200, X200 Tablet, X200s, X200t, X201, X201 Tablet, X201i, X201s, X201si, X201T, X220, X220 Tablet, X220i, X220i Tablet, X230, X230S, X230T, X230 Tablet, X240, X240S, X250, X260, X270, X280, X300, X301, X380, X380 Yoga, X380 Yoga S1, X390, X390 YOGA, X395, X41, X41 Tablet, X60, X60 Tablet, X60s, X61, X61 Tablet, X61s, XYoga 260, YOGA 11E 2ND GEN, YOGA 11E 3RD GEN, YOGA 11E 4TH GEN, YOGA 11E 5TH GEN, YOGA 12, YOGA 14, YOGA 260, YOGA 370, YOGA 460
ThinkPad Z Series	Z61P, Z61T
ThinkBook Series	13s, 14, 14s, 15

<https://www.absolute.com/partners/device-compatibility/#lenovo>

The electronic devices are operable to support various operating systems including Windows 10 and macOS 10.13.

Is my device compatible with Absolute Home & Office?

A: We currently support devices running Windows 10 or macOS 10.13 (High Sierra) or higher.

Unfortunately, we are no longer able to officially provide support for older versions of operating systems. While our software may install successfully, it has only been tested on the above operating system versions, and technical issues may arise with installations on older operating systems.

At this time, we do not offer support for iOS or Android mobile devices.

<https://homeoffice.absolute.com/support/faq/#toggle-id-5>

	The electronic devices connect to the internet and communicate with a server system. As stated in Absolute's Lojack For Laptops FAQs ("LFL FAQs"), "Absolute Software hosts the Absolute Monitoring Center [including a server] in a co-location hosting facility owned by Telus Corporation." LoJack for Laptops (paperzz.com) at p. 5. "If you can browse, then LoJack for Laptops will work. Our goal is as close to zero-configuration as possible....LoJack for Laptops will work using any DSL, wireless, or cable internet service provider. We are also compatible with most Satellite ISPs." LFL FAQs at p. 5.
--	--

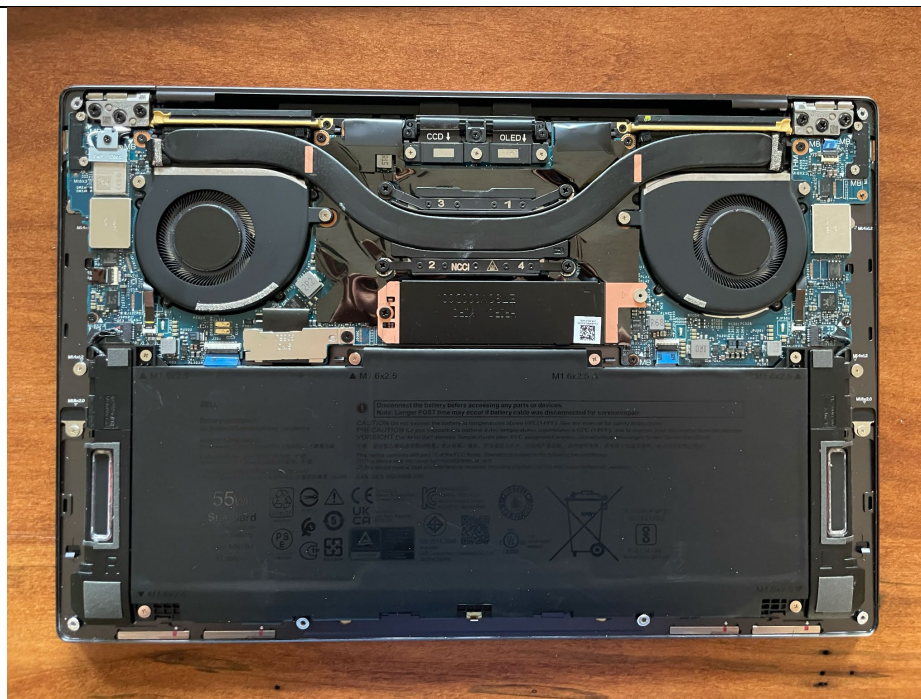
	Where is my data stored? Absolute Software hosts the Absolute Monitoring Center in a co-location hosting facility owned by Telus Corporation. The Telus facility provides restricted access security, redundant high-speed access to the internet and redundant power supply to the Absolute Monitoring Center. Absolute has implemented a full backup and restore plan with nightly backups stored on a separate server and weekly offsite backups. Absolute has mandated a maximum down-time of 4 hours for website access and a maximum of 24 hours to restore the Agent communications server for a site-contained catastrophic event. What if your server is unavailable when the Agent tries to call? If the Computrace Agent in your computer is unable to connect to the Monitoring Server during its regularly scheduled time, it will attempt to call every 15 minutes until successful. How do I know that the Monitoring Center is safeguarded against access to unauthorized users? We have implemented numerous safeguards to restrict unauthorized access to the Absolute Monitoring Center. The Absolute Monitoring server can only be accessed via client-initiated Computrace Agent communications. Access requires two-way authentication ensuring only valid Computrace Agents can access the server. All Agent communications are encrypted with RC4 128-bit encryption. CONNECTIVITY Can the Computrace Agent in LoJack for Laptops work through firewalls (including personal firewalls) to reach the internet? If you can browse, then LoJack for Laptops will work. Our goal is as close to zero-configuration as possible. What kind of internet connection should I use? LoJack for Laptops will work using any DSL, wireless, or cable internet service provider. We are also compatible with most Satellite ISPs. <i>Id.</i>
[1a] a processor;	The Accused Instrumentalities comprise “a processor.” A laptop has a processor (e.g., a CPU) and one or more non-transitory machine-readable storage media responsive to the processor (e.g., any of various memory units in the laptop including ROM, RAM, cache, and storage). When Computrace/Lojack for Laptops is installed on the laptop, it constitutes a security

application in at least one of the non-transitory machine-readable storage media operable to perform the following operations.



Internals of laptop used for experiments

	The Computrace Agent consists of two components: <u>Application Agent</u>: Installed in the operating system (as a service) by running an installer. It makes regularly scheduled calls over the internet to the Absolute Monitoring Center and provides asset and location data on each Agent call. The Application Agent also manages the Absolute “helper applications” to support activities like data delete commands or to aid in theft recovery. <u>Persistence Module</u>: Installed in the BIOS (or the firmware) of most laptops at the factory and activated during the Application Agent’s first call to the Absolute Monitoring Center. It restores the Application Agent if it’s removed. For example, if a thief steals a computer and reinstalls the operating system, the Persistence Module restores the Agent. The Persistence Module remains dormant until the Application Agent is installed. Lojack for Laptops FAQ (LFL FAQ) at 1. https://paperzz.com/doc/7965781/lojack-for-laptops
[1b] one or more non-transitory machine-readable storage media responsive to the processor; and	The Accused Instrumentalities comprise “one or more non-transitory machine-readable storage media responsive to the processor.” Testing confirms that the Accused Instrumentalities include a computer system that includes a central processing unit (processor). The device used for performing the experiments on the Absolute software is pictured below, which shows that it has a processor and memory (one or more non-transitory machine readable storage media).

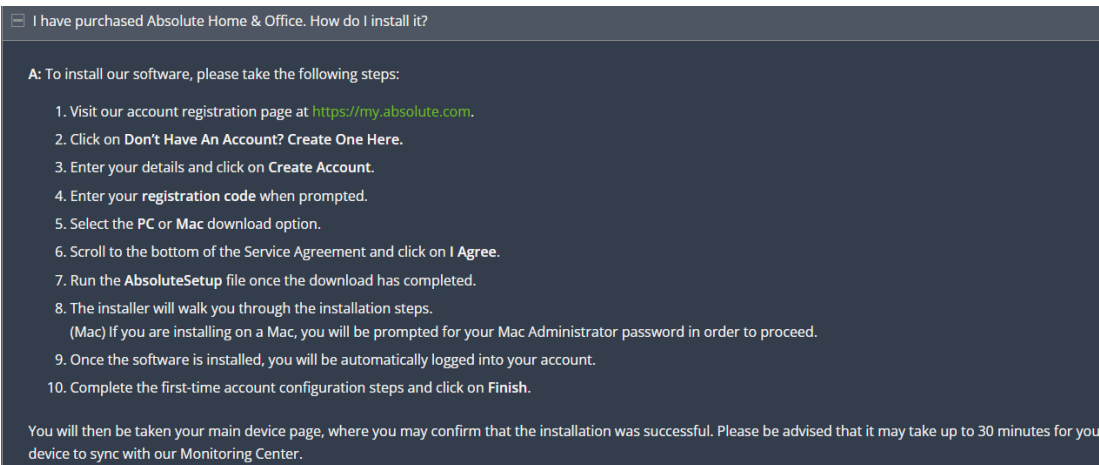


Internals of laptop used for experiments

[1c] a security application in at least one of the non-transitory machine-readable storage media, wherein the security application is operable to perform operations comprising:	The Accused Instrumentalities comprise “a security application in at least one of the non-transitory machine-readable storage media, wherein the security application is operable to perform operations comprising.” The Computrace Agent consists of two components: <u>Application Agent</u>: Installed in the operating system (as a service) by running an installer. It makes regularly scheduled calls over the internet to the Absolute Monitoring Center and provides asset and location data on each Agent call. The Application Agent also manages the Absolute “helper applications” to support activities like data delete commands or to aid in theft recovery. <u>Persistence Module</u>: Installed in the BIOS (or the firmware) of most laptops at the factory and activated during the Application Agent’s first call to the Absolute Monitoring Center. It restores the Application Agent if it’s removed. For example, if a thief steals a computer and reinstalls the operating system, the Persistence Module restores the Agent. The Persistence Module remains dormant until the Application Agent is installed. Lojack for Laptops FAQ (LFL FAQ) at 1. https://paperzz.com/doc/7965781/lojack-for-laptops On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element. As detailed in the remaining claim elements the security applications performs the claimed features.
[1d] enabling an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers;	The Accused Instrumentalities comprise “enabling an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element.

Testing confirms that the software contains instructions operable to enable an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers.

For example, Absolute provides a website with a URL (<https://my.absolute.com>) with an Account Registration Page where a user can enter a registration code to register the mobile electronic device with the Home & Office security service.



<https://homeoffice.absolute.com/support/faq/#toggle-id-11>

Absolute Home & Office is a security service at least partially residing on one or more servers.

What is the difference between Absolute Home & Office Basic, Standard and Premium?

A: **Absolute Home & Office Basic** offers the ability to view your device's location on a map, remotely lock your device, and remotely delete some or all files from your device.

Absolute Home & Office Standard offers all the features above. In addition, if your laptop is stolen, you may report it to us and our team of investigators will work with law enforcement to track down and recover the device.

Absolute Home & Office Premium offers all of the above, and additionally includes our \$1000 Service Guarantee: if we are not able to recover your stolen laptop, you may then be eligible for a payment of up to \$1000. Please note that the Premium edition of Home & Office is only sold in our guaranteed recovery territories (the United States, Canada, the United Kingdom and Australia.)

You may find more details on our Product Comparison page (<https://homeoffice.absolute.com/product-comparison/>).

<https://homeoffice.absolute.com/support/faq/#toggle-id-1>

The “Application Component... makes regularly scheduled calls over the internet to the Absolute Monitoring Center [the server system] and provides asset and location data on each Agent call.” LFL FAQs at p. 1.

COMPUTRACE AGENT

What is the Computrace® Agent?

The Computrace Agent is the part of our LoJack® for Laptops technology that resides within your computer. It maintains contact with the Absolute Monitoring Center. In the event of theft, we can communicate with the Agent to determine the location of your computer, who has it, and what they're doing with it.

The Computrace Agent consists of two components:

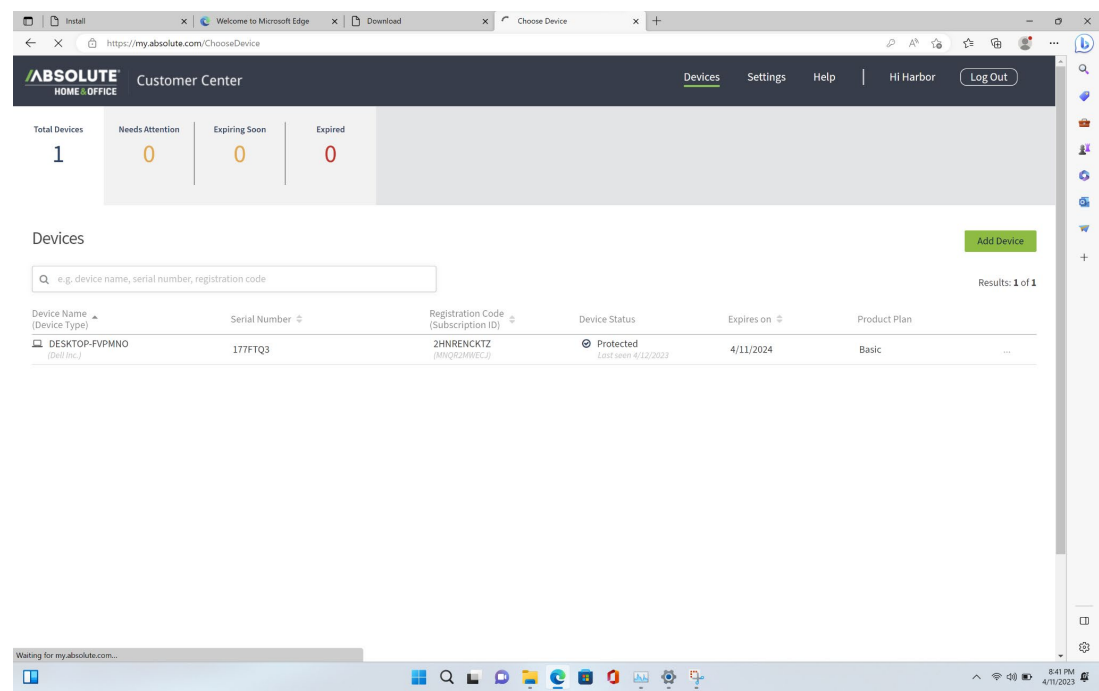
Application Agent: Installed in the operating system (as a service) by running an installer. It makes regularly scheduled calls over the internet to the Absolute Monitoring Center and provides asset and location data on each Agent call. The Application Agent also manages the Absolute “helper applications” to support activities like data delete commands or to aid in theft recovery.

Persistence Module: Installed in the BIOS (or the firmware) of most laptops at the factory and activated during the Application Agent's first call to the Absolute Monitoring Center. It restores the Application Agent if it's removed. For example, if a thief steals a computer and reinstalls the operating system, the Persistence Module restores the Agent. The Persistence Module remains dormant until the Application Agent is installed.

———— **Absolute**® Software ————

Id.

Analysis of the Absolute web interface confirms the Accused Instrumentalities include the claim limitation. Once an electronic device has been registered with the security service, the web interface shows the user that the electronic device is protected.



Absolute web interface UI

Clicking on the electronic device row navigates the user to an administrative web interface for the electronic device. Within the web interface, the user has different administrative security options that the user can take for the electronic device such as locking, locating, erasing, recovering, removing license.

ABSOLUTE

HOME OFFICE

Customer Center

DevicesSettingsHelpHi HarborLog Out

Protected

DESKTOP-FVPMNO

Dell Inc.

SupportRemove License

LocateLockEraseRecover

Serial Number

177FTQ3

Make and Model

Dell Inc. XPS 9320

Device Status

Protected

Last seen 4/13/2023

Product Plan

Basic

License Status

Active

Expires on

4/11/2024

Registration Code

2HNRENCKTZ

Device Billing

Most recent location

18 hours ago.

Disable Locate

© 2023 Absolute Software Corporation. All rights reserved. Privacy Policy | Service Agreement | Patents in US, CAN, UK, GER, AUS, JPN

Keyboard shortcutsMap data ©2023Terms of UseReport a map error

For support issues, visit Absolute Global Support.

Absolute web service showing that a user can administer the security service for the electronic device

Absolute utilizes a client/server architecture. Therefore, the Accused Instrumentalities include a server system.

	<i>Chapter 1: Introduction</i> Absolute® brings a fundamentally new approach to cybersecurity by enabling self-healing endpoint security to ensure uncompromised visibility and near real-time remediation of breaches at the source. Our cloud-based platform and embedded Persistence technology puts IT and security professionals in control of devices, data, and applications — whether they are on or off the network — to improve IT asset management, ensure compliance, protect data, and reduce insider threats. Patented Persistence technology is embedded in the firmware of more than 1 billion popular PC and mobile devices from global manufacturers including Acer, Asus, Dell, Fujitsu, HP, Intel, Lenovo, Microsoft, Panasonic, Samsung and Toshiba. Absolute is an adaptive endpoint security solution. Its technology platform is a client/server architecture that delivers device security, data security, and asset management of endpoints, even if a device is off the network or in the hands of an unauthorized user. The persistent connection between the secure and patented agent (client) and the Absolute Monitoring Center (server) ensures organizations have protected access to up-to-date information about their entire device inventory. Authorized users can use the built-in tools in the Absolute console to track devices and initiate data and device security operations for the purposes of enforcing compliance policies, identifying at-risk computers, and taking preemptive and reactive measures if a security incident occurs. https://help.absolute.com/corporate/html5/en/Content/PDFs/EN/AbsoluteUG.en.pdf
[1e] causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service;	The Accused Instrumentalities comprise “causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element. Testing confirms that the Absolute software contains instructions operable to cause the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service. For example, the software “makes regularly scheduled calls over the internet to the Absolute Monitoring Center [security service] and provides asset and location data [identifying information for the mobile electronic

	device] to support activities like data delete commands or to aid in theft recovery.” LFL FATS at 1. For further example, Lojack automatically transmits the “results of a comprehensive system scan, IP address, user- and machine names and location data” to the server system “once a day.”
--	---

LoJack for Laptops

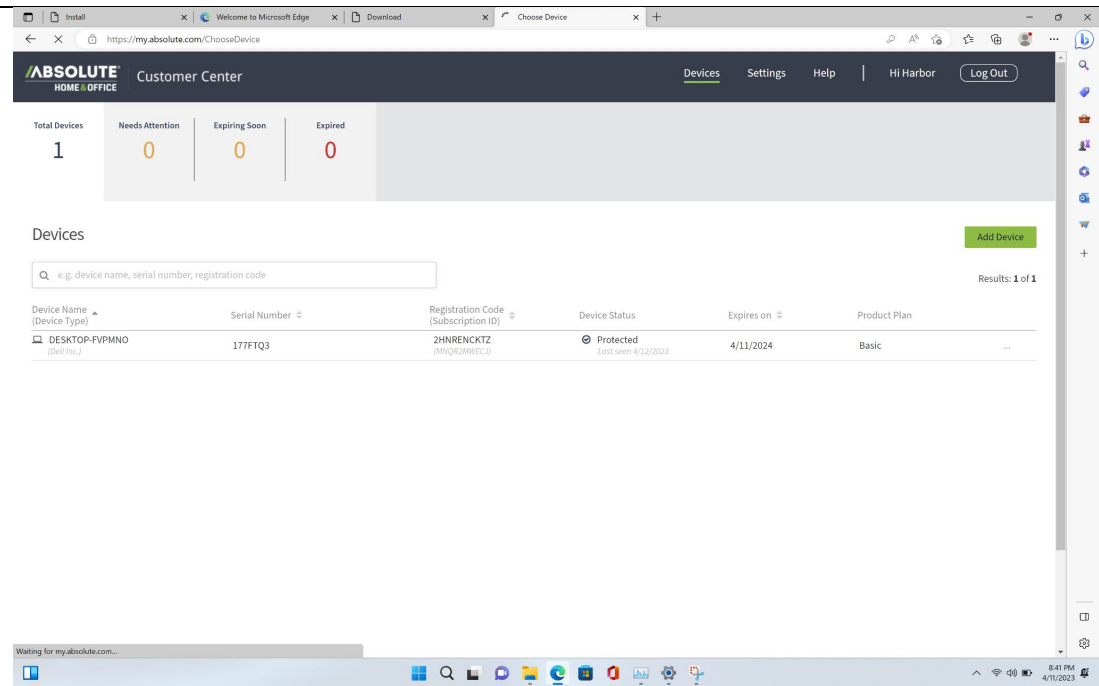
A software product from Vancouver, British Columbia, based Absolute Software that enables law enforcement to recover stolen [laptops](#) by tracing them via the Internet.^{[9][10]} The product was initially sold under the name "Computrace". In 2005, Absolute Software licensed the LoJack brand name and produces the software under both the Computrace and "LoJack for Laptops" product names.^[11] Unlike the LoJack for vehicles and equipment products, which use a small radio beacon installed in the tracked device, the Computrace/LoJack for Laptops product is [laptop tracking software](#) that periodically [phones home](#) to Absolute Software's server to both announce its location and to check to see if the machine has been reported stolen.^{[12][13]} *LoJack* comes preinstalled in the [BIOSes](#) of, at least, Lenovo, HP, [Dell](#), [Fujitsu](#), Panasonic, [Toshiba](#), and [Asus](#) machines.^[14] It is disabled by default and can be enabled by purchasing a license for *Computrace*; upon being enabled, the BIOS will copy a downloader named `rpcnetp.exe` from the BIOS flash ROM to %WINDIR%\System32 (which usually resolves to C:\WINDOWS\System32) which will in turn download the actual agent `rpcnet.exe` and install it as a [windows service](#). Recently^[when?], Dell, Lenovo, Panasonic and Fujitsu appear to have discontinued this method and require manual installation.^[citation needed] Once enabled, *Computrace* cannot be disabled or deinstalled without assistance from *Absolute Software*, not even by reformatting or substituting the hard disk, because the BIOS keeps reinstalling or repairing it prior to loading the [operating system](#).

From then on, `rpcnet.exe` will phone home to *Absolute Software* servers once a day, querying for a possible theft report, and, in any case, transmitting the results of a comprehensive system scan, IP address, user- and machine names and location data, which it obtains either by tapping the GPS data stream on machines equipped with GPS hardware, or by triangulating available [WLAN](#) access points in the vicinity, by providing WLAN IDs and signal strengths so *Absolute Software* servers can geolocate the device using the [Mexens Technology](#) data base.^[citation needed]

If *Absolute* receives a theft report, the service can be remotely commanded to phone home every 15 minutes, install additional 3rd vendor software, such as a key logger or a forensic package, make [screenshots](#), etc.

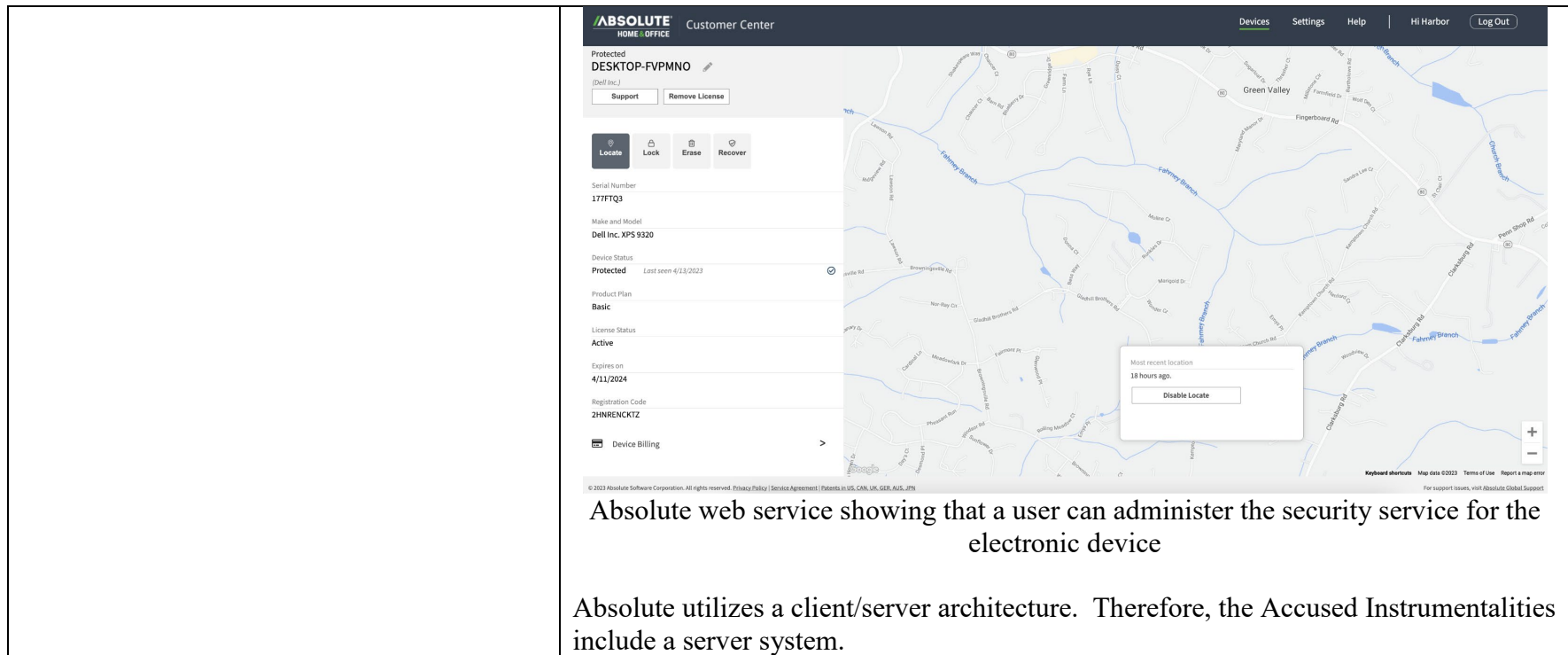
Computrace also supports [Intel's AT-p](#) anti theft protection scheme: If it is unable to phone home within a configurable time interval it will require a special BIOS password upon the next reboot. It can be configured to shut down the machine's power supply immediately in this case, to force a reboot.

<https://en-academic.com/dic.nsf/enwiki/1378022>



Absolute web interface UI

Clicking on the electronic device row navigates the user to an administrative web interface for the electronic device. Within the web interface, the user has different administrative security options that the user can take for the electronic device such as locking, locating, erasing, recovering, removing license.



Absolute web service showing that a user can administer the security service for the electronic device

Absolute utilizes a client/server architecture. Therefore, the Accused Instrumentalities include a server system.

	<i>Chapter 1: Introduction</i> Absolute® brings a fundamentally new approach to cybersecurity by enabling self-healing endpoint security to ensure uncompromised visibility and near real-time remediation of breaches at the source. Our cloud-based platform and embedded Persistence technology puts IT and security professionals in control of devices, data, and applications — whether they are on or off the network — to improve IT asset management, ensure compliance, protect data, and reduce insider threats. Patented Persistence technology is embedded in the firmware of more than 1 billion popular PC and mobile devices from global manufacturers including Acer, Asus, Dell, Fujitsu, HP, Intel, Lenovo, Microsoft, Panasonic, Samsung and Toshiba. Absolute is an adaptive endpoint security solution. Its technology platform is a client/server architecture that delivers device security, data security, and asset management of endpoints, even if a device is off the network or in the hands of an unauthorized user. The persistent connection between the secure and patented agent (client) and the Absolute Monitoring Center (server) ensures organizations have protected access to up-to-date information about their entire device inventory. Authorized users can use the built-in tools in the Absolute console to track devices and initiate data and device security operations for the purposes of enforcing compliance policies, identifying at-risk computers, and taking preemptive and reactive measures if a security incident occurs. https://help.absolute.com/corporate/html5/en/Content/PDFs/EN/AbsoluteUG.en.pdf
[1f] after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to periodically communicate with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;	The Accused Instrumentalities comprise “after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to periodically communicate with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element. Testing confirms that before the owner has registered the mobile electronic device, the software is “disabled by default and can be enabled by purchasing a license for Computrace.” “Once enabled,” the LoJack software “will phone home to Absolute Software servers once a day.”

LoJack for Laptops

A software product from Vancouver, British Columbia, based Absolute Software that enables law enforcement to recover stolen [laptops](#) by tracing them via the Internet.^{[9][10]} The product was initially sold under the name "Computrace". In 2005, Absolute Software licensed the LoJack brand name and produces the software under both the Computrace and "LoJack for Laptops" product names.^[11] Unlike the LoJack for vehicles and equipment products, which use a small radio beacon installed in the tracked device, the Computrace/LoJack for Laptops product is [laptop tracking software](#) that periodically [phones home](#) to Absolute Software's server to both announce its location and to check to see if the machine has been reported stolen.^{[12][13]} *LoJack* comes preinstalled in the [BIOSes](#) of, at least, Lenovo, HP, [Dell](#), [Fujitsu](#), Panasonic, [Toshiba](#), and [Asus](#) machines.^[14] It is disabled by default and can be enabled by purchasing a license for *Computrace*; upon being enabled, the BIOS will copy a downloader named `rpcnetp.exe` from the BIOS flash ROM to %WINDIR%\System32 (which usually resolves to C:\WINDOWS\System32) which will in turn download the actual agent `rpcnet.exe` and install it as a [windows service](#). Recently^[when?], Dell, Lenovo, Panasonic and Fujitsu appear to have discontinued this method and require manual installation.^[citation needed] Once enabled, *Computrace* cannot be disabled or deinstalled without assistance from *Absolute Software*, not even by reformatting or substituting the hard disk, because the BIOS keeps reinstalling or repairing it prior to loading the [operating system](#).

From then on, `rpcnet.exe` will phone home to *Absolute Software* servers once a day, querying for a possible theft report, and, in any case, transmitting the results of a comprehensive system scan, IP address, user- and machine names and location data, which it obtains either by tapping the GPS data stream on machines equipped with GPS hardware, or by triangulating available [WLAN](#) access points in the vicinity, by providing WLAN IDs and signal strengths so *Absolute Software* servers can geolocate the device using the [Mexens Technology](#) data base.^[citation needed]

If *Absolute* receives a theft report, the service can be remotely commanded to phone home every 15 minutes, install additional 3rd vendor software, such as a key logger or a forensic package, make [screenshots](#), etc.

Computrace also supports [Intel's AT-p](#) anti theft protection scheme: If it is unable to phone home within a configurable time interval it will require a special BIOS password upon the next reboot. It can be configured to shut down the machine's power supply immediately in this case, to force a reboot.

<https://en-academic.com/dic.nsf/enwiki/1378022>

I just received my new laptop. Is Absolute Home & Office already installed?

A: Although you may have purchased an Absolute Home & Office license bundled with your device, it is important to note that vendors do not pre-install our software, and you will need to install and activate Home & Office yourself.

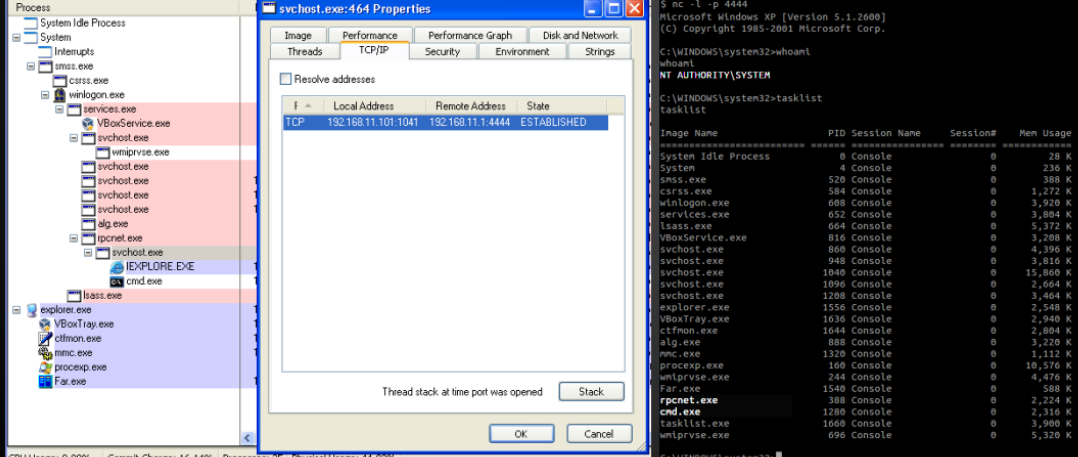
Different vendors will fulfill an Absolute Home & Office product purchase in different ways. If you have any questions on how this product will be delivered to you, we recommend that you [contact our Global Support Department](#), or reach out to the vendor you purchased it from originally. Most vendors should provide you with a **registration code**, which you will need to create your account and activate your device.

If your laptop is older and you aren't sure if you ever installed a purchased Absolute Home & Office license, please contact us with your device's serial number and we would be happy to provide you with more information.

“Unlike the LoJack for vehicles and equipment products, which use a small radio beacon installed in the tracked device, the Computrace/LoJack for Laptops product is laptop tracking software that periodically phones home to Absolute Software's server to both announce its location and to check to see if the machine has been reported stolen.[12][13] “

<https://en-academic.com/dic.nsf/enwiki/1378022>

When Computrace agent connects to a control **server** it updates to a more secure main agent **rpcnet.exe**. The main agent implements security checks which prevent simple RCE. However, implementation has weakness and allows to easily override security settings which enables arbitrary code execution again. DEMO!



The screenshot displays a Windows XP desktop environment. On the left, the 'Process' window shows a tree view of running processes, with 'svchost.exe' highlighted. In the center, the 'svchost.exe:464 Properties' dialog box is open, showing the 'Performance' tab. On the right, a command prompt window shows the output of the 'tasklist' command, listing various system processes and their memory usage. The output includes processes like System Idle Process, System, smss.exe, csrss.exe, winlogon.exe, services.exe, lsass.exe, VBoxService.exe, vmtoolsd.exe, explorer.exe, VBoxTray.exe, notepad.exe, process.exe, Far.exe, rpcnet.exe, cmd.exe, tasklist.exe, and vmtoolsd.exe.

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Console	0	28 K
System	4	Console	0	236 K
smss.exe	520	Console	0	388 K
csrss.exe	584	Console	0	1,272 K
winlogon.exe	688	Console	0	3,920 K
services.exe	652	Console	0	3,804 K
lsass.exe	664	Console	0	5,372 K
VBoxService.exe	816	Console	0	3,208 K
svchost.exe	860	Console	0	4,396 K
svchost.exe	948	Console	0	3,816 K
svchost.exe	1040	Console	0	15,860 K
svchost.exe	1096	Console	0	2,664 K
svchost.exe	1288	Console	0	3,464 K
explorer.exe	1556	Console	0	2,548 K
VBoxTray.exe	1636	Console	0	2,940 K
ctfmon.exe	1644	Console	0	2,804 K
alg.exe	888	Console	0	3,220 K
mmc.exe	1320	Console	0	1,112 K
process.exe	160	Console	0	10,576 K
vmtoolsd.exe	244	Console	0	4,476 K
Far.exe	1540	Console	0	588 K
rpcnet.exe	388	Console	0	2,224 K
cmd.exe	1280	Console	0	2,316 K
tasklist.exe	1660	Console	0	3,900 K
vmtoolsd.exe	696	Console	0	5,328 K

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Computrace-Backdoor-Revisited.pdf>

[illegible]

35

Communication explained

COMPUTRACISH:

```

1. c
2. s 7e ff ff ff ff 04 00 e5 de 00 70 08 96 e8 7e
3. c 7e e5 de 00 70 04 00 c0 fe 88 00 09 a9 f0 7e
4. s 7e ff ff ff ff 04 00 e5 de 00 70 19 94 f8 7e
5. c 7e e5 de 00 70 e5 de 00 70 84 00 c0 fe 88 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6. s 7e c0 fe 88 00 0c 00 2a b7 be 7e
7. c 7e e5 de 00 70 e5 de 00 70 0c 00 02 00 a4 03 05
01 28 0a 00 f0 73 00 2b 45 16 7e
8. s 7e c8 fe 88 00 04 00 3b 8f a2 7e
9. c 7e e5 de 00 70 e5 de 00 70 04 00 00 f0 73 00 3c
45 8c 7e
  
```

ENGLISH:

Hi

Hello. My name is 0x7000dee5

Oh, 0x7000dee5, do you understand me? You can control me via 0x0088fec0

Hello. My name is 0x7000dee5

0x7000dee5, 0x7000dee5, haven't you just said it twice? I know what you mean! :-)

Show me what you got in your control structure (0x0088fec0)

Sure thing, take it: 02 00 a4 03 05 01 28 0a 00 f0 73 00

Nice, nice. Can you show me what you have at 0x0088fec8 once again?

It's all yours: 0x0073f000

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Computrace-Backdoor-Revisited.pdf>

Communication explained

COMPUTRACISH:

```
10. s 7e cc fe 88 00 0c 00 07 00 00 00 0c 93 00 00 d4
fe 88 00 4c 45 40 7e
11. c 7e e5 de 00 70 e5 de 00 70 04 00 a4 3c 1b 00 4d
46 04 7e
12. s 7e ac 3c 1b 00 02 00 78 05 5d c7 e6 7e
13. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 5e
67 f1 7e
14. s 7e d8 fe 88 00 04 00 ac 3c 1b 00 6e 93 68 7e
15. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 6f
41 83 7e
16. s 7e 3a 42 1b 00 02 00 78 05 7f 5b 1f 7e
17. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 78
23 55 7e
```

ENGLISH:

Ok, lets allocate 0x930c bytes of memory. Please put result of this operation here: 0x0088fed4

No troubles, man! Here is the location: 0x001b3ca4

How do you know I am a man? Anyway, let me teach you to read long messages. We will enlarge your buffer to process larger requests. This size should be enough: 0x0578

Yeah.. sorry, I didn't mean... Lets do that!

Good, then here is the new buffer address for input requests: 0x001b3cac.

Acknowledged.

Use same buffer size 0x0578 for output processing as well.

Of course! I do what you say.

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Comptrace-Backdoor-Revisited.pdf>

Communication explained

COMPUTRACISH:

```

18. s 7e dc fe 88 00 04 00 08 7f 2f 7e
19. c 7e e5 de 00 70 e5 de 00 70 04 00 28 fd 88 00 09
03 c6 7e
20. s 7e 2c fd 88 00 04 00 19 9c 47 7e
21. c 7e e5 de 00 70 e5 de 00 70 04 00 e5 de 00 70 1a
05 66 7e
22. s 7e 3e 42 1b 00 04 00 e5 de 00 70 2a 09 5d 7e
23. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 2b
49 c3 7e
24. s 7e 32 42 1b 00 04 00 e5 de 00 70 3b f8 84 7e
25. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 3c
2b 15 7e
26. s 7e dc fe 88 00 04 00 3a 42 1b 00 4c cd 2f 7e
27. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 4d
45 a3 7e
  
```

ENGLISH:

Remind your output processing structure address.

That's easy: 0x0088fd28

Time to check if you are lying. What's the SessionId of that output processing structure?

Well.. I guess you know, it's 0x7000dee5

Alright, you're doing good. Then use it in new output processing.

Absolutely! ^.^

Ok, new communication structure is ready at 0x001b423a

You are a magician! Now I can chat without any limits!.. I really appreciate what you do. It's amazing. I wanted to tell you one story about[end of buffer]

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-CompuTrace-Backdoor-Revisited.pdf>

[1g] after the owner has registered the mobile electronic device with the security service, accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or

The Accused Instrumentalities comprise after the owner has registered the mobile electronic device with the security service, accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device.

requested disabling of the mobile electronic device;	On information and belief, review of Absolute's source code review will further demonstrate that the Accused Instrumentalities perform this claim element. Testing and documentation confirm that "[o]nce enabled," the Absolute software "phones home to Absolute Software's server to both announce its location and to check to see if the machine has been reported stolen." Part of phoning home includes "querying for a possible theft report [message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device."
--	--

LoJack for Laptops

A software product from Vancouver, British Columbia, based Absolute Software that enables law enforcement to recover stolen [laptops](#) by tracing them via the Internet.^{[9][10]} The product was initially sold under the name "Computrace". In 2005, Absolute Software licensed the LoJack brand name and produces the software under both the Computrace and "LoJack for Laptops" product names.^[11] Unlike the LoJack for vehicles and equipment products, which use a small radio beacon installed in the tracked device, the Computrace/LoJack for Laptops product is [laptop tracking software](#) that periodically [phones home](#) to Absolute Software's server to both announce its location and to check to see if the machine has been reported stolen.^{[12][13]} *LoJack* comes preinstalled in the [BIOSes](#) of, at least, Lenovo, HP, [Dell](#), [Fujitsu](#), Panasonic, [Toshiba](#), and [Asus](#) machines.^[14] It is disabled by default and can be enabled by purchasing a license for *Computrace*; upon being enabled, the BIOS will copy a downloader named `rpcnetp.exe` from the BIOS flash ROM to %WINDIR%\System32 (which usually resolves to C:\WINDOWS\System32) which will in turn download the actual agent `rpcnet.exe` and install it as a [windows service](#). Recently^[when?], Dell, Lenovo, Panasonic and Fujitsu appear to have discontinued this method and require manual installation.^[citation needed] Once enabled, *Computrace* cannot be disabled or deinstalled without assistance from *Absolute Software*, not even by reformatting or substituting the hard disk, because the BIOS keeps reinstalling or repairing it prior to loading the [operating system](#).

From then on, `rpcnet.exe` will phone home to *Absolute Software* servers once a day, querying for a possible theft report, and, in any case, transmitting the results of a comprehensive system scan, IP address, user- and machine names and location data, which it obtains either by tapping the GPS data stream on machines equipped with GPS hardware, or by triangulating available [WLAN](#) access points in the vicinity, by providing WLAN IDs and signal strengths so *Absolute Software* servers can geolocate the device using the [Mexens Technology](#) data base.^[citation needed]

If *Absolute* receives a theft report, the service can be remotely commanded to phone home every 15 minutes, install additional 3rd vendor software, such as a key logger or a forensic package, make [screenshots](#), etc.

Computrace also supports [Intel's AT-p](#) anti theft protection scheme: If it is unable to phone home within a configurable time interval it will require a special BIOS password upon the next reboot. It can be configured to shut down the machine's power supply immediately in this case, to force a reboot.

<https://en-academic.com/dic.nsf/enwiki/1378022>

With Absolute Home & Office Basic, a user can “remotely lock [their] device.” With Absolute Home & Office Standard and Premium, a user “may report [a theft] to us and

our team of investigators will work with law enforcement to track down and recover the device.”

What is the difference between Absolute Home & Office Basic, Standard and Premium?

A: Absolute Home & Office Basic offers the ability to view your device's location on a map, remotely lock your device, and remotely delete some or all files from your device.

Absolute Home & Office Standard offers all the features above. In addition, if your laptop is stolen, you may report it to us and our team of investigators will work with law enforcement to track down and recover the device.

Absolute Home & Office Premium offers all of the above, and additionally includes our \$1000 Service Guarantee: if we are not able to recover your stolen laptop, you may then be eligible for a payment of up to \$1000. Please note that the Premium edition of Home & Office is only sold in our guaranteed recovery territories (the United States, Canada, the United Kingdom and Australia.)

You may find more details on our Product Comparison page (<https://homeoffice.absolute.com/product-comparison/>).

<https://homeoffice.absolute.com/support/faq/#toggle-id-10-closed>

My device has been stolen! How do I report the theft to Absolute?

A: To report the theft of your device and open a theft file with us, please take the following steps:

1. Report the theft to your local police and obtain a police file number.
 1. Please note that this police file number is required, as we cannot take any action without it.
2. Contact our Theft Reporting Support Department to report the theft over the phone. We offer theft reporting services by phone 24 hours a day, 7 days a week.
 1. Alternately, you may log into your account at <https://my.absolute.com> and click on the Recover tab to submit an online theft report.
 2. If you are calling from outside of North America, a full list of contact numbers is available at <http://homeoffice.absolute.com/en/support/global-telephone-support>.

Please note that we will require the following information to open your theft file:

Police file number
Name of police department
Non-emergency phone number for police department
Date of theft
Address of theft
A description of how the theft occurred

<https://homeoffice.absolute.com/support/faq/#toggle-id-65>

How do I deploy an Absolute Lock?

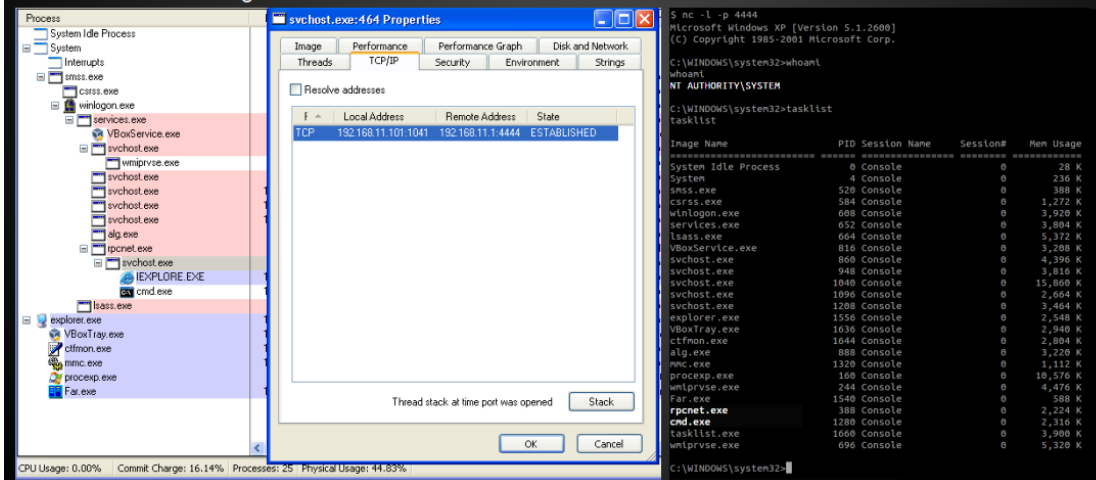
A: To deploy an Absolute Lock to your registered device, please take the following steps:

1. Visit our login page at <https://my.absolute.com> and enter your registered email address.
 1. If you do not remember the password on this account, click on the **Forgot Password** link to have a new temporary password emailed to you.
 2. If you used a temporary password to log in, update to a permanent password.
2. If you have multiple devices, select the correct one from the list.
3. Click on **Lock**.
4. Enter a lock message to be displayed on your device.
5. Enter your 4-6 number PIN code.
6. Confirm that you understand that the device will need to be unlocked prior to requesting a recovery.
7. Click on **Lock Device**.

Your Lock request will be deployed the next time the device contacts our Monitoring Center.

<https://homeoffice.absolute.com/support/faq/#toggle-id-41>

When Computrace agent connects to a control **server** it updates to a more secure main agent **rpcnet.exe**. The main agent implements security checks which prevent simple RCE. However, implementation has weakness and allows to easily override security settings which enables arbitrary code execution again. DEMO!



The screenshot displays a Windows XP desktop environment. On the left, the 'Process' window shows a tree view of running processes, with 'svchost.exe' highlighted. In the center, the 'svchost.exe:464 Properties' dialog box is open, showing the 'Performance' tab. On the right, a command prompt window shows the output of the 'tasklist' command, listing various system processes and their memory usage. The output includes:

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Console	0	28 K
System	4	Console	0	236 K
smss.exe	520	Console	0	388 K
csrss.exe	584	Console	0	1,272 K
winlogon.exe	608	Console	0	3,920 K
services.exe	652	Console	0	3,804 K
lsass.exe	664	Console	0	5,372 K
VBoxService.exe	816	Console	0	3,208 K
svchost.exe	860	Console	0	4,396 K
svchost.exe	948	Console	0	3,816 K
svchost.exe	1040	Console	0	15,808 K
svchost.exe	1096	Console	0	2,664 K
svchost.exe	1288	Console	0	3,464 K
explorer.exe	1556	Console	0	2,548 K
VBoxTray.exe	1636	Console	0	2,940 K
ctfmon.exe	1644	Console	0	2,804 K
alg.exe	888	Console	0	3,220 K
mmc.exe	1320	Console	0	1,112 K
proccexp.exe	160	Console	0	10,576 K
wmprvse.exe	244	Console	0	4,476 K
Far.exe	1540	Console	0	388 K
rpcnet.exe	388	Console	0	2,224 K
cmd.exe	1280	Console	0	2,316 K
tasklist.exe	1660	Console	0	3,900 K
wmprvse.exe	696	Console	0	5,328 K

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Computrace-Backdoor-Revisited.pdf>

[illegible]

43

Communication explained

COMPUTRACISH:

1. c
2. s 7e ff ff ff ff 04 00 e5 de 00 70 08 96 e8 7e
3. c 7e e5 de 00 70 04 00 c0 fe 88 00 09 a9 f0 7e
4. s 7e ff ff ff ff 04 00 e5 de 00 70 19 94 f8 7e
5. c 7e e5 de 00 70 e5 de 00 70 84 00 c0 fe 88 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6. s 7e c0 fe 88 00 0c 00 2a b7 be 7e
7. c 7e e5 de 00 70 e5 de 00 70 0c 00 02 00 a4 03 05
01 28 0a 00 f0 73 00 2b 45 16 7e
8. s 7e c8 fe 88 00 04 00 3b 8f a2 7e
9. c 7e e5 de 00 70 e5 de 00 70 04 00 00 f0 73 00 3c
45 8c 7e

ENGLISH:

Hi

Hello. My name is 0x7000dee5

Oh, 0x7000dee5, do you understand me? You can control me via 0x0088fec0

Hello. My name is 0x7000dee5

0x7000dee5, 0x7000dee5, haven't you just said it twice? I know what you mean! :-)

Show me what you got in your control structure (0x0088fec0)

Sure thing, take it: 02 00 a4 03 05 01 28 0a 00 f0 73 00

Nice, nice. Can you show me what you have at 0x0088fec8 once again?

It's all yours: 0x0073f000

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Computrace-Backdoor-Revisited.pdf>

Communication explained

COMPUTRACISH:

```
10. s 7e cc fe 88 00 0c 00 07 00 00 00 0c 93 00 00 d4
fe 88 00 4c 45 40 7e
11. c 7e e5 de 00 70 e5 de 00 70 04 00 a4 3c 1b 00 4d
46 04 7e
12. s 7e ac 3c 1b 00 02 00 78 05 5d c7 e6 7e
13. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 5e
67 f1 7e
14. s 7e d8 fe 88 00 04 00 ac 3c 1b 00 6e 93 68 7e
15. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 6f
41 83 7e
16. s 7e 3a 42 1b 00 02 00 78 05 7f 5b 1f 7e
17. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 78
23 55 7e
```

ENGLISH:

Ok, lets allocate 0x930c bytes of memory. Please put result of this operation here: 0x0088fed4

No troubles, man! Here is the location: 0x001b3ca4

How do you know I am a man? Anyway, let me teach you to read long messages. We will enlarge your buffer to process larger requests. This size should be enough: 0x0578

Yeah.. sorry, I didn't mean... Lets do that!

Good, then here is the new buffer address for input requests: 0x001b3cac.

Acknowledged.

Use same buffer size 0x0578 for output processing as well.

Of course! I do what you say.

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Comptrace-Backdoor-Revisited.pdf>

Communication explained

COMPUTRACISH:

```

18. s 7e dc fe 88 00 04 00 08 7f 2f 7e
19. c 7e e5 de 00 70 e5 de 00 70 04 00 28 fd 88 00 09
    03 c6 7e
20. s 7e 2c fd 88 00 04 00 19 9c 47 7e
21. c 7e e5 de 00 70 e5 de 00 70 04 00 e5 de 00 70 1a
    05 66 7e
22. s 7e 3e 42 1b 00 04 00 e5 de 00 70 2a 09 5d 7e
23. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 2b
    49 c3 7e
24. s 7e 32 42 1b 00 04 00 e5 de 00 70 3b f8 84 7e
25. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 3c
    2b 15 7e
26. s 7e dc fe 88 00 04 00 3a 42 1b 00 4c cd 2f 7e
27. c 7e e5 de 00 70 e5 de 00 70 04 00 02 00 a4 03 4d
    45 a3 7e
  
```

ENGLISH:

Remind your output processing structure address.

That's easy: 0x0088fd28

Time to check if you are lying. What's the SessionId of that output processing structure?

Well.. I guess you know, it's 0x7000dee5

Alright, you're doing good. Then use it in new output processing.

Absolutely! ^.^

Ok, new communication structure is ready at 0x001b423a

You are a magician! Now I can chat without any limits!.. I really appreciate what you do. It's amazing. I wanted to tell you one story abou[end of buffer]

<https://www.blackhat.com/docs/us-14/materials/us-14-Kamlyuk-Kamluk-Computrace-Backdoor-Revisited.pdf>

“Unlike the LoJack for vehicles and equipment products, which use a small radio beacon installed in the tracked device, the Computrace/LoJack for Laptops product is laptop tracking software that periodically phones home to Absolute Software's server to both announce its location and to check to see if the machine has been reported stolen.[12][13] “

<https://en-academic.com/dic.nsf/enwiki/1378022>

[1h] in response to receiving the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and	The Accused Instrumentalities comprise “in response to receiving the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element. Documentation confirms that when a user locks the device, the device is locked from all user functions. For example, Task Manager is not available, “making it essentially impossible for anyone to use your device.” The device, however, still is able to communicate with the security service to, e.g., unlock the device. Locking Your Device In case of theft or loss of your device, you can disable your device using the Lock feature. Performing a lock remotely locks the screen of your device. No Windows application, even Task Manager, is available, making it essentially impossible for anyone to use your device. Even if someone reinstalls the operating system, your device still remains locked. Only you can unlock your device. https://help.absolute.com/html5/en/Content/New%20Consumer%20Web%20Help/Section_3/Locking/LockingDevice.htm
---	---

How do I remove an Absolute Lock?

A: To remove an Absolute Lock from your registered device, please take the following steps:

1. Visit our login page at <https://my.absolute.com> and enter your registered email address.
 1. If you do not remember the password on this account, click on the **Forgot Password** link to have a new temporary password emailed to you.
 2. If you used a temporary password to log in, update to a permanent password.
2. If you have multiple devices, select the correct one from the list.
3. Click on **Lock**.
4. Enter your 4-6 number **PIN code** (the same code used when you locked your device).
5. Click on **Unlock Device**.

Please note that you will need to connect the device to the Internet before it can be unlocked. If you require an immediate unlock of a locked device, please [contact our Global Support Department](#) directly.

<https://homeoffice.absolute.com/support/faq/#toggle-id-42>

Absolute Computrace features a “remote poison pill” which “locks down OS and prevents boot.” PC-Disable Whitepaper at p. 1. This “remote poison pill” is triggered in response to a notification [from Absolute’s Monitoring Center] that the computer has been reported stolen.

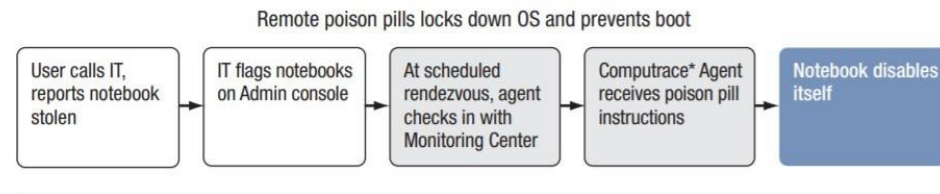
Through Computrace, an authorized information technology (IT) administrator can remotely delete data on a notebook, or the notebook can now intelligently lock itself down and prevent an OS from booting. If the notebook is reported lost or stolen, the IT administrator simply flags it in the Computrace Web portal and sets up a “poison pill” so the next time the notebook “phones home,” it will be disabled. In both cases, whether the notebook locks itself down or receives a poison pill, and even if the hard drive is reformatted or replaced, anti-theft security options remain in place. Getting the system operational again is easy – authorized users can quickly restore the system with a one-time reactivation token provided by the IT department.

<https://wenku.baidu.com/view/7d4803717fd5360cba1adbef.html>

“Computrace allows a remote lock-down of a notebook as soon as the system connects to the Internet and checks in with the Absolute Monitoring Center. If the notebook’s theft flag has been set in the server database, the poison pill is delivered

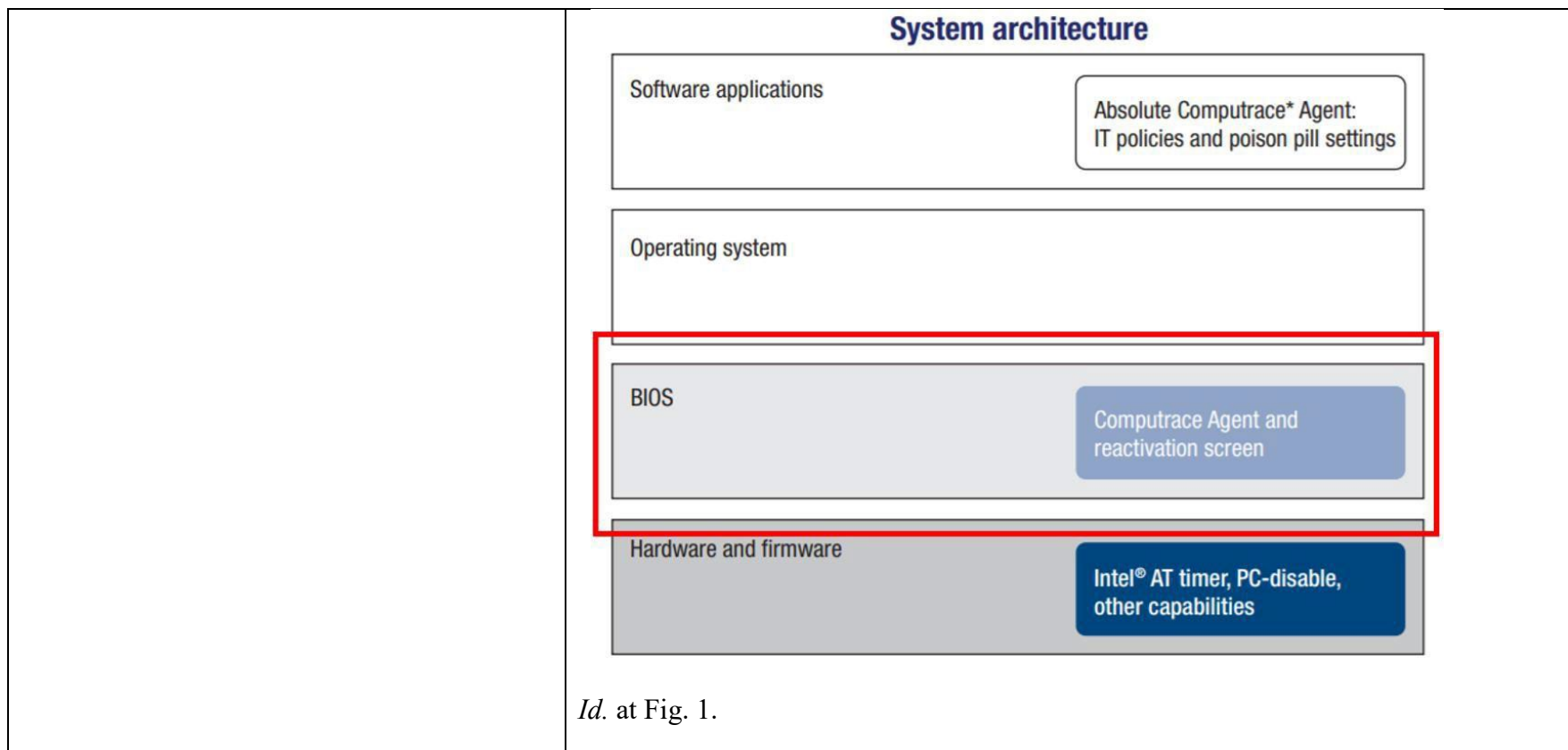
when the notebook checks in. The notebook then disables itself and prevents the OS from rebooting. Even if the hard drive is replaced, the notebook will not boot. Only the reactivation screen is available.” <https://manualzz.com/doc/23910598/pc-disable-delivers-intelligent-client>

**Use cases for Absolute Software Computrace*
with Intel® Anti-Theft Technology**



Id.

Computrace’s PC-Disable feature relies on a BIOS security component.



How Absolute solutions help you protect your data

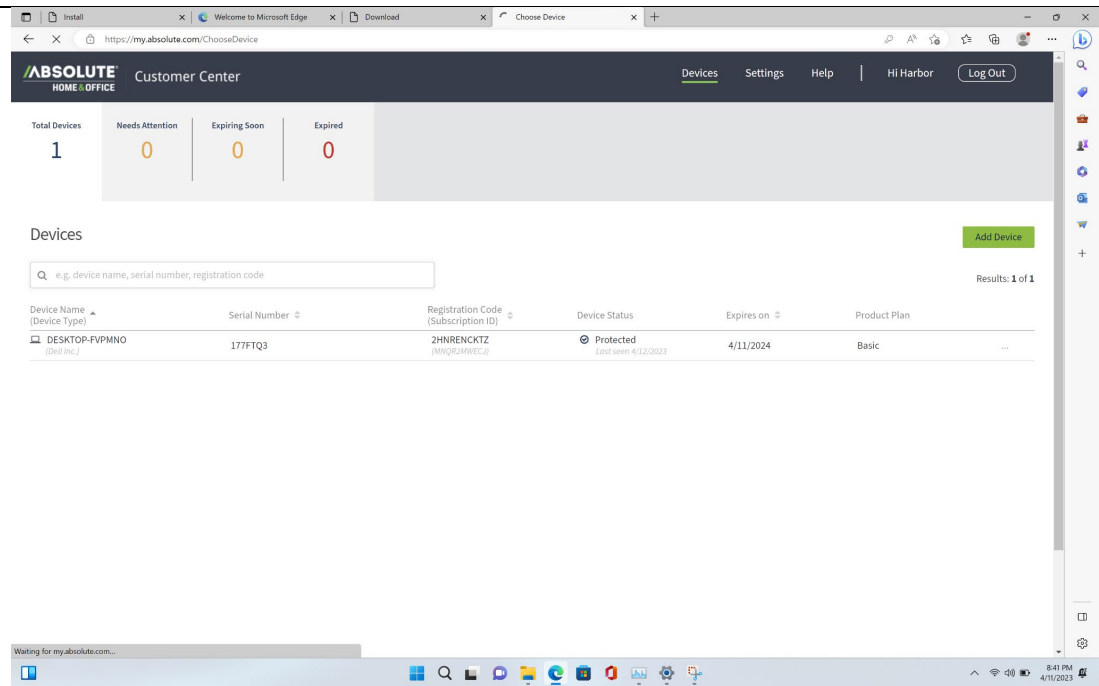
The Absolute Investigations Team is dedicated to working with law enforcement to find and return stolen laptops. Using a direct, two-way connection between the Absolute solution and the laptop, our laptop tracker solutions don't only try to locate your laptop, they help customers remotely erase their data through their security console. Part of feeling secure when your laptop goes missing isn't just about laptop recovery, it's knowing that whatever personal data is on there isn't going to fall into the wrong hands. Read a few of their highlighted recovery stories:

Absolute Investigations Monthly Roundup: Device Recovery Stories

Absolute Resilience is more than remote device management—it includes automated, self-healing tools and people who specialize in recovering laptops. And if they can't, you can make any data on the machine unusable.

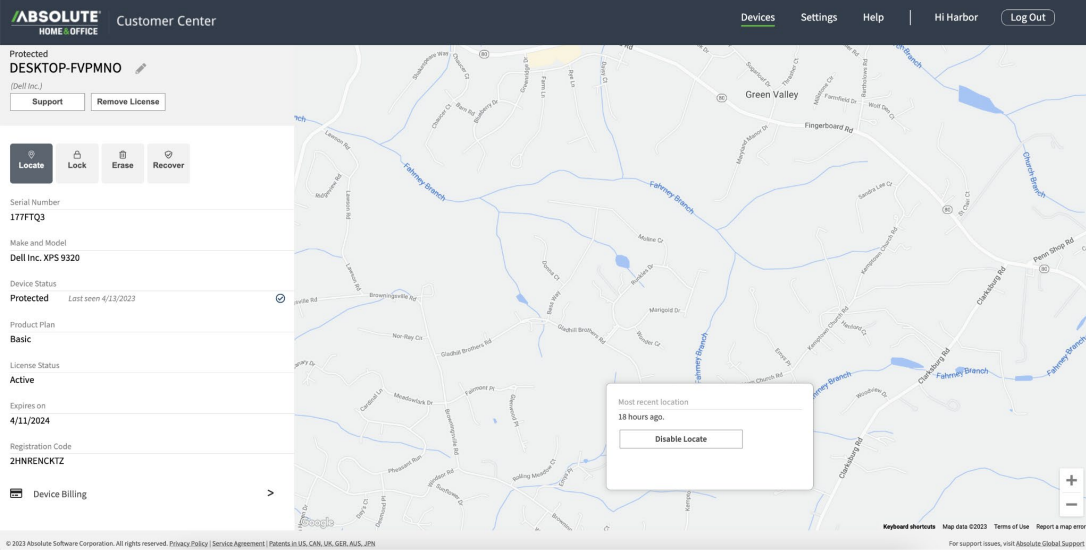
<https://www.absolute.com/blog/how-to-guide-tracking-and-recovering-laptops/>

Analysis of the Absolute web interface confirms the Accused Instrumentalities include the claim limitation. Once an electronic device has been registered with the security service, the web interface shows the user that the electronic device is protected.



Absolute web interface UI

Clicking on the electronic device row navigates the user to an administrative web interface for the electronic device. Within the web interface, the user has different administrative security options that the user can take for the electronic device such as locking, locating, erasing, recovering, removing license.

	 Absolute web service showing that a user can administer the security service for the electronic device
[1i] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;	The Accused Instrumentalities comprise “automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element. Documentation, as discussed above, Lojack automatically transmits the “results of a comprehensive system scan, IP address, <i>user-</i> and machine <i>names</i> and location data” to the server system “once a day.”

	I am concerned about privacy issues. What kind of information do you collect from my computer? Standard communication between your computer and our Monitoring Center occurs once a day and consists of basic information like memory size, hard drive size, type of processor, type of operating system, user name, IP and Mac addresses. There is no active monitoring of your computer until you report a theft. After a theft is reported, your computer will contact our Monitoring Center every 15 minutes. This increased contact allows the Absolute Theft Recovery Team to obtain specific details about where your computer is located, who is using it, and what they're doing with it. LFL FAQ at 4.
--	---

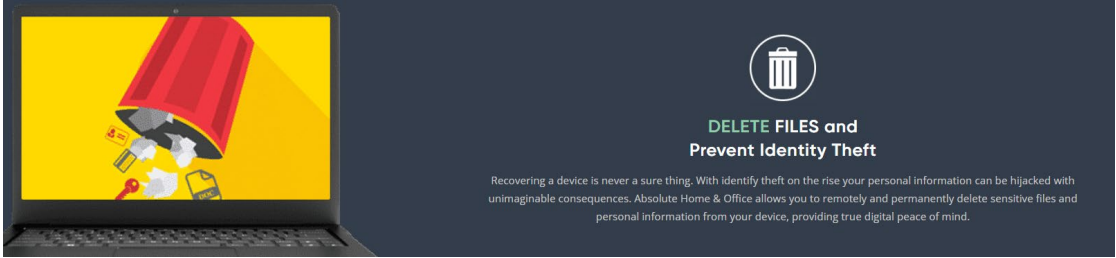
Classic File List and File Retrieval:

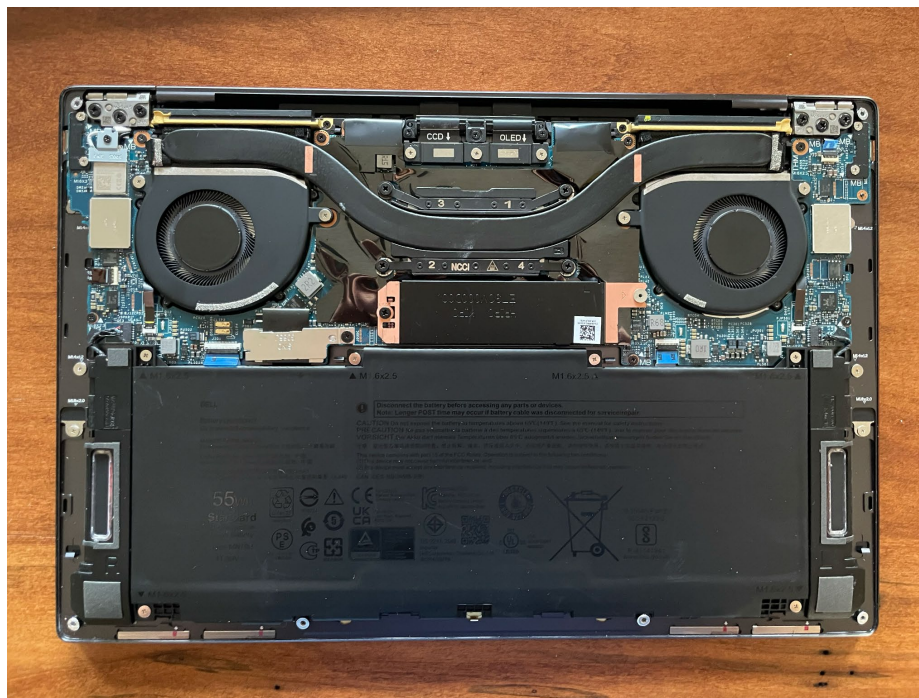
We are in the process of retiring the Classic File List and File Retrieval features across all customers. Certain customers can still access the features through the 'File List Summary Report' and 'File Retrieval Summary Report' respectively under the 'Settings' pane of the console. Both reports will be completely retired across all customers on March 4th. Going forward, please utilize the following four Absolute Reach scripts as replacements for the retired Classic features:

Replacing the Classic File Retrieval feature:

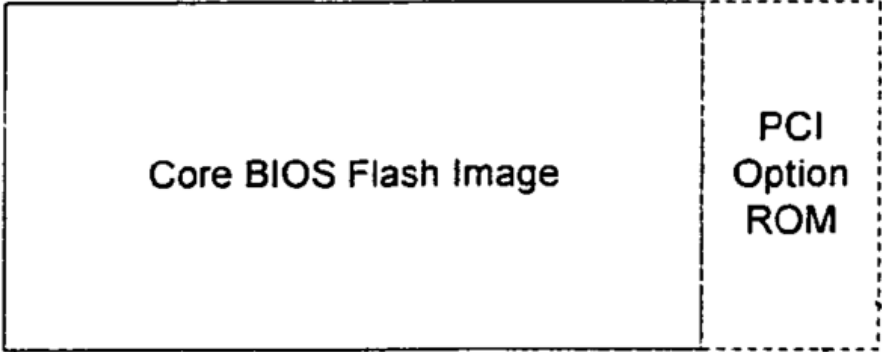
- Upload files to Dropbox
- Upload files to FTP server
- Upload files to network shared folder

<https://community.absolute.com/s/article/Product-Update-End-of-Life-of-Classic-Absolute-Features>

	Vancouver, Canada: December 7, 2010 – Absolute® Software Corporation (“Absolute” or the “Company”) (TSX: ABT), the leading provider of firmware-based, patented, computer theft recovery, data protection and secure computer lifecycle management solutions announced today that its SaaS computer tracking solution Computrace® now includes Remote File Retrieval. With this new data leakage prevention (DLP) feature, IT administrators can use the Computrace cloud to identify and retrieve sensitive company files that are exposed on end point devices. This can be done proactively to mitigate the risk of data loss, or as an emergency response action on missing or stolen devices prior to remotely wiping the hard drive for complete corporate data security. In addition to being an exciting new security feature in Computrace, the Remote File Retrieval (RFR) feature can be an essential productivity tool. For example, a travelling executive works on a confidential PowerPoint presentation on the plane, but leaves her laptop in a cab on the way to her hotel. Once notified, IT may be able to remotely retrieve the lost file and send it to the executive in time for her partner meetings. https://www.absolute.com/company/press-releases/2010/absolute-empowers-it-with-new-data-leakage-prevention-capabilities/  https://homeoffice.absolute.com/features/
[1j] wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;	The Accused Instrumentalities comprise “wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory.” At least part of the instructions for the Absolute software are stored in read-only memory (ROM) relating to the basic input-output system (BIOS). For example, testing confirms that the Accused Instrumentalities include a computer system that includes a memory that is programmed and a processor that executes those programmed instructions. The device used for performing the experiments on the Absolute software is pictured below, which shows that it has a memory (RAM and a hard drive) and a processor.



Internals of laptop used for experiments

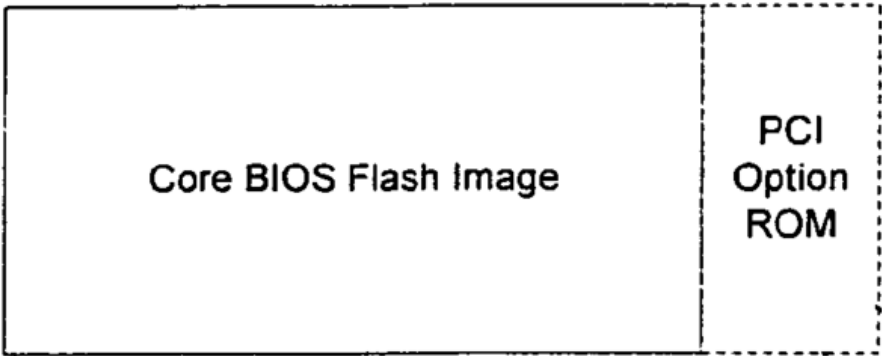
	3. Computrace Agent Normal Operation Computrace Agent is a Windows application that has two variants: a small agent and a full-size agent. The Small Agent is a piece of code that is of minimal possible size and maximum extensibility. This module is embedded into BIOS PCI Option ROM or UEFI firmware. According to the US patent 20060272020 by Absolute Software, where it is called a mini CDA (Communications Driver Agent), it was designed to check if the full-function agent is installed and functioning on the system, and if not, load the full function CDA across the Internet from the server. According to the patent, the persistence module resides in BIOS Option ROM:  https://securelist.com/absolute-computrace-revisited/58278/ The Application agent is stored on memory, which is also non-volatile memory.
[1k] wherein the non-volatile memory comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user;	The Accused Instrumentalities comprise “wherein the non-volatile memory comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element.

Documentation and testing confirm that depending on administrative settings and user permissions, an operating system and file system, stored in non-volatile memory, either provide access to certain files (e.g., files stored in a changeable area) or restrict access to certain files (e.g., files stored in a system area that cannot be modified by a user). The Application agent is not changeable by a user and therefore resides at least partially in the system area.

3. Computrace Agent Normal Operation

Computrace Agent is a Windows application that has two variants: a small agent and a full-size agent. The Small Agent is a piece of code that is of minimal possible size and maximum extensibility. This module is embedded into BIOS PCI Option ROM or UEFI firmware. According to the [US patent 20060272020](#) by Absolute Software, where it is called a mini CDA (Communications Driver Agent), it was designed to check if the full-function agent is installed and functioning on the system, and if not, load the full function CDA across the Internet from the server.

According to the patent, the persistence module resides in BIOS Option ROM:



<https://securelist.com/absolute-computrace-revisited/58278/>

[11] wherein the security application utilizes code residing at least partially in the system area; and	The Accused Instrumentalities comprise “wherein the security application utilizes code residing at least partially in the system area.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element. Documentation confirms the presence of this feature. ABSOLUTE PLATFORM AGENT Since Persistence relies on the presence of the Absolute platform agent, how easily can it be detected? The software agent is tamper-resistant and difficult to detect. It runs as a non-descript service and is not listed as an application, nor does it show up on the programs menu listing or as a system tray icon. https://www.absolute.com/media/2467/faq-absolute-persistence-absolute-software.pdf What is the footprint, or size, of the Computrace Agent? The Computrace Agent has a very small footprint, requiring less than 200Kb of disk space. It occupies a small Absolute[®]Software FAQ amount of memory when idle, and when placing a call the Agent optimizes data transfer, which means a very low demand is placed on the network.
--	---

<https://paperzz.com/doc/7965781/lojack-for-laptops>

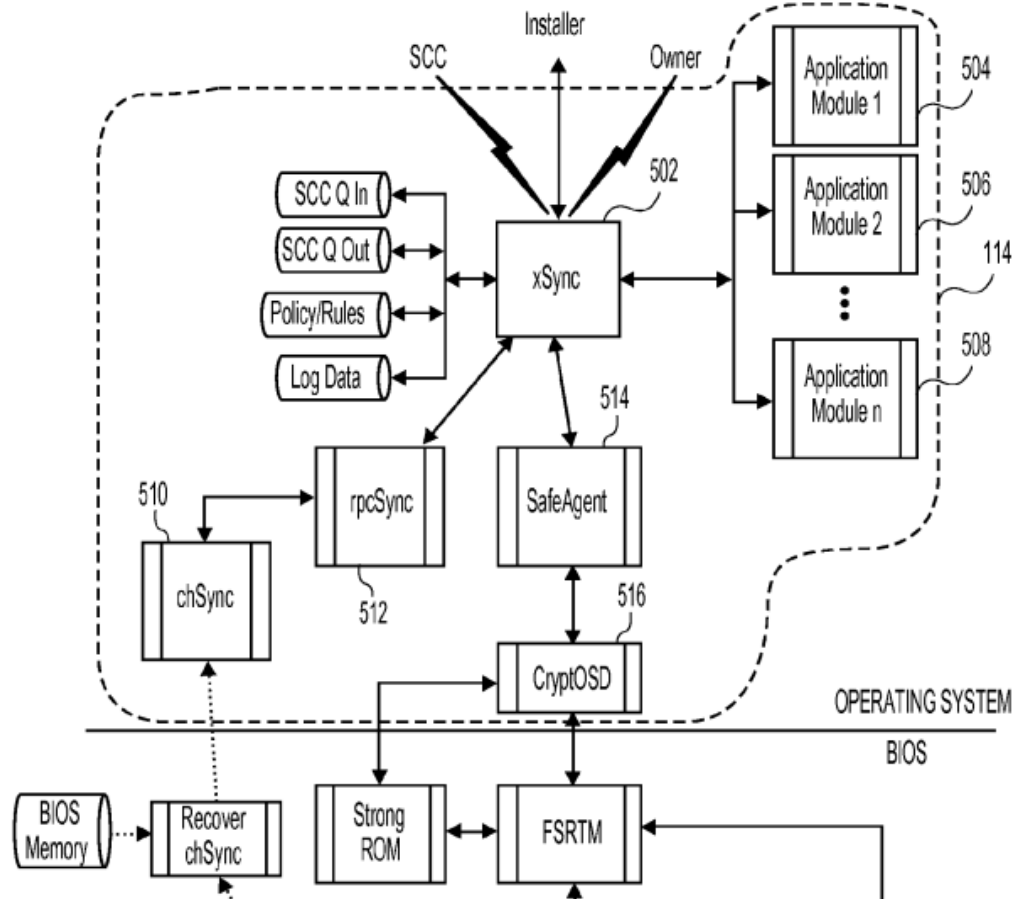
Upon information and belief, Absolute Home & Office practices U.S. Patent 8,745,383 (“the ’383 patent”). For example, Absolute Software Corporation includes the ’383 patent in disclosures of IP on press releases.

©2015 Absolute Software Corporation. All rights reserved. Computrace and Absolute are registered trademarks of Absolute Software Corporation. LoJack is a registered trademark of LoJack Corporation, used under license by Absolute Software Corporation. LoJack Corporation is not responsible for any content herein. U.S. patents No. 5,715,174, No. 5,896,497, No. 6,087,937, No. 6,958,688 No. 7,818,557, No. 7,818,803, No. 7,945,709, No. 8,062,380, No. 8,234,359, No. 8,241,369, No. 8,307,055, No. 8,332,953, No. 8,346,234, No. 8,362,901, No. 8,418,226, No. 8,419,806, No. 8,441,348, No. 8,510,825, No. 8,556,991, No. 8,566,961, No. 8,625,799, No. 8,669,870, No. 8,701,013, No. 8,712,432, No. 8,717,172, No. 8,734,529, No. 8,745,383, No. 8,800,061, No. 8,868,933, No. 8,878,672, No. 8,902,066, and No. 8,904,523. Canadian patents No. 2,211,735, No. 2,284,806, No. 2,205,370, No. 2,771,208 and No. 2,733,222. U.K. patents No. EP0793823, No. GB2298302, and No. GB2338101. German patent No. 69512534. Australian patent No. 699045, No. 2009279430, No. 2009279431, No. 2010315412, No. 2010324789, and No. 2010321633. Japanese patents No. 4067035, No. 5220924, No. 5475743, No. 5363305, and No. 5508502. Korean patents No. 10-1372986 and No. 10-1408746. Mexican patents No. 297,406 and No. 306,287. Russian patent No. 2,460,220 and 2,506,704. The Toronto Stock Exchange has neither approved nor disapproved of the information contained in this news release.

<https://www.prnewswire.com/news-releases/absolute-software-to-use-google-maps-geolocation-api-to-track-devices-287624131.html>

See also <https://www.absolute.com/company/legal/patents/>

The ’383 patent describes a component in the form of chSync 510 and CryptOSD 516, both shown in Figure 5A, reproduced in part below.



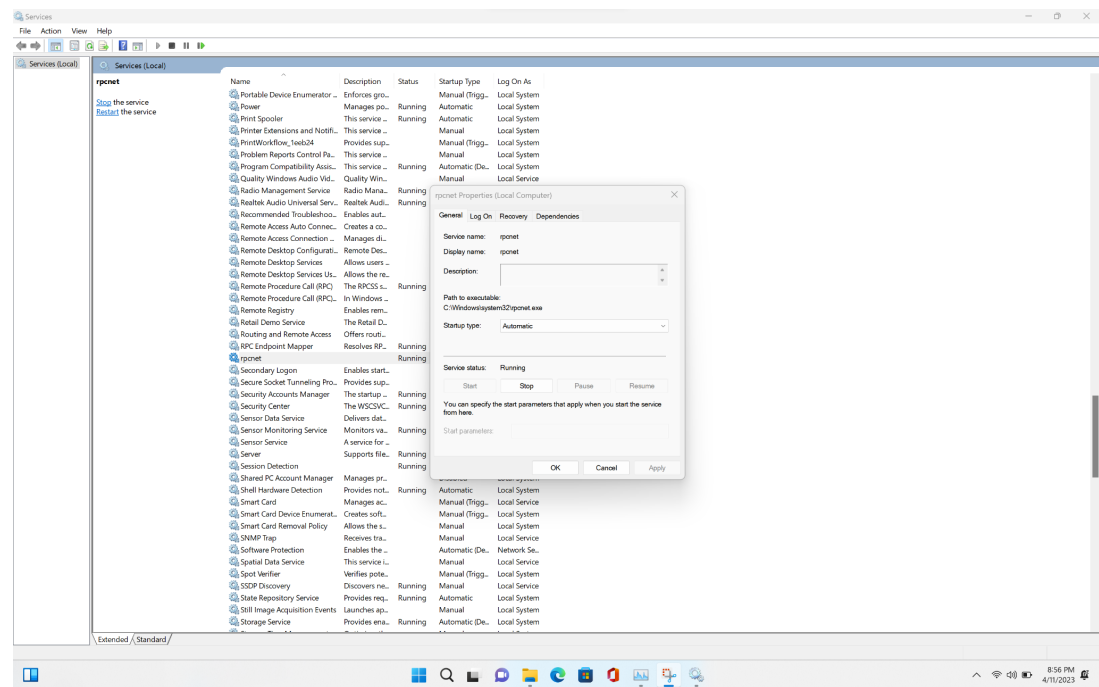
The chSync module is a component. For example, in Figure 5A the chSync module is illustrated as operating behind the scenes of user interaction with the operating system (e.g., it is not an application module that users would interact with).

The chSync module contains a validator module capable of determining whether the application component is present and whether the application component has been tampered with. For example, “chSync module 510 is also responsible for determining

	whether rpcSync module 512 is installed and uncorrupted, and if not, chSync module 510 is responsible for installing rpcSync module 512.” ’383 patent, 11:30-33. Upon information and belief, the application module comprises at least the xSync module, the rpcSync module, and the SafeAgent. As another example, “chSync module 410 checks the process and file status of rpcSync module 412 and xSync module 402 and records their status for SafeAgent module’s 414 use in forming the heartbeat message. xSync module 402 also checks the process/file status of SafeAgent module 414, CryptOSD module 416, and all xSync applications modules 404, 406, and 408 and records their status for SafeAgent module’s 414 use in forming the heartbeat message.” ’383 patent, 12:62-13:3. The Computrace system is capable of determining whether the application component has been tampered with. Tampering can include deleting the application module, operating system re-installations, hard drive reformat and hard drive replacements. As discussed in FAQs at LFL FAQs at pp. 2-3: What if an unauthorized user still manages to delete the Computrace Agent? Our Agent employs a self-healing technology referred to as “persistence” that allows the Computrace BIOS-module (when the computer manufacturer embeds the Computrace Persistence Module into the BIOS or firmware of your computer) to essentially rebuild the Application Agent software even if the service is deleted. What if I want to remove the Computrace Agent in Lojack for Laptops from my computer? If the Agent has been activated and you are an authorized user with the correct password, you can submit a request to have the Agent removed from your computer. <i>Id.</i> Upon information and belief, rpcnetp is configured to make this determination. This is supported by V. Kamlyuk, S. Belov and A. Sacco, “Absolute Backdoor Revisited,” BlackHat, June 2014. [Online]. Available: https://www.blackhat.com/docs/us-14/materials/us-14-Kamluk-Computrace-Backdoor-Revisited-WP.pdf (last accessed April 27, 2023) (hereafter “Absolute
--	--

Backdoor Revisited”). Absolute Backdoor Revisited, which is further confirmed with analysis of Absolute’s software.

After locating the rpcnet.exe windows service, its execution can be terminated. This would then disable the absolute software from maintaining a connection with the servers.



rpcnet windows service Image

Once the process is terminated, the rpcnetp service begins execution in order to download and reinstall the rpcnetp service from the server.

Name	Status	CPU	Memory	Disk	Network
Microsoft® Volume Shadow Copy Service		0%	1.2 MB	0 MB/s	0 Mbps
PC Doctor Dell SupportAssist API		0%	86.8 MB	0 MB/s	0 Mbps
Realtek HD Audio Universal Service		0%	2.5 MB	0 MB/s	0 Mbps
Realtek HD Audio Universal Service		0%	2.5 MB	0 MB/s	0 Mbps
Realtek HD Audio Universal Service		0%	3.3 MB	0 MB/s	0 Mbps
rpcnetp (32 bit)		0%	1.3 MB	0 MB/s	0 Mbps
rpcnetp		0%	1.1 MB	0 MB/s	0 Mbps
Runtime Broker		0%	1.0 MB	0 MB/s	0 Mbps
Runtime Broker		0%	1.0 MB	0 MB/s	0 Mbps
SessionService		0%	0.4 MB	0 MB/s	0 Mbps
Sink to receive asynchronous callbacks for WMI client application		0%	0.7 MB	0 MB/s	0 Mbps
Spooler SubSystem App		0%	3.7 MB	0 MB/s	0 Mbps
Start (2)		0.1%	31.8 MB	0.1 MB/s	0 Mbps
svchost.exe		0.8%	2.7 MB	0.1 MB/s	0.1 Mbps
Touch Keyboard and Handwriting Panel		0%	2.0 MB	0 MB/s	0 Mbps
Usermode Font Driver Host		0%	1.5 MB	0 MB/s	0 Mbps
Usermode Font Driver Host		0%	1.3 MB	0 MB/s	0 Mbps
Waves Audio Service		0%	2.4 MB	0 MB/s	0 Mbps
Waves MaxxAudio Service Application		0.1%	112.8 MB	0 MB/s	0 Mbps
WavesSysSvc Service Application		0%	13.3 MB	0 MB/s	0 Mbps
Widgets (7)		0.2%	152.4 MB	0.8 MB/s	0 Mbps
Windows Audio Device Graph Isolation		0%	1.6 MB	0 MB/s	0 Mbps
Windows Defender SmartScreen		0%	1.0 MB	0 MB/s	0 Mbps
Windows Driver Foundation - User-mode Driver Framework Host ...		0%	8.9 MB	0 MB/s	0 Mbps
Windows Driver Foundation - User-mode Driver Framework Host ...		0%	1.3 MB	0 MB/s	0 Mbps
Windows Driver Foundation - User-mode Driver Framework Host ...		0.2%	8.7 MB	0 MB/s	0 Mbps
Windows Input Experience (3)		0.8%	21.6 MB	1.5 MB/s	0.1 Mbps
Windows Modules Installer		0%	1.0 MB	0 MB/s	0 Mbps
Windows Security Health Service		0%	1.9 MB	0 MB/s	0 Mbps
Windows Security notification icon		0%	0.9 MB	0 MB/s	0 Mbps
Windows Service Wrapper		0%	2.7 MB	0 MB/s	0 Mbps
Windows Wireless LAN 802.11 Extensibility Framework		0%	0.9 MB	0 MB/s	0 Mbps

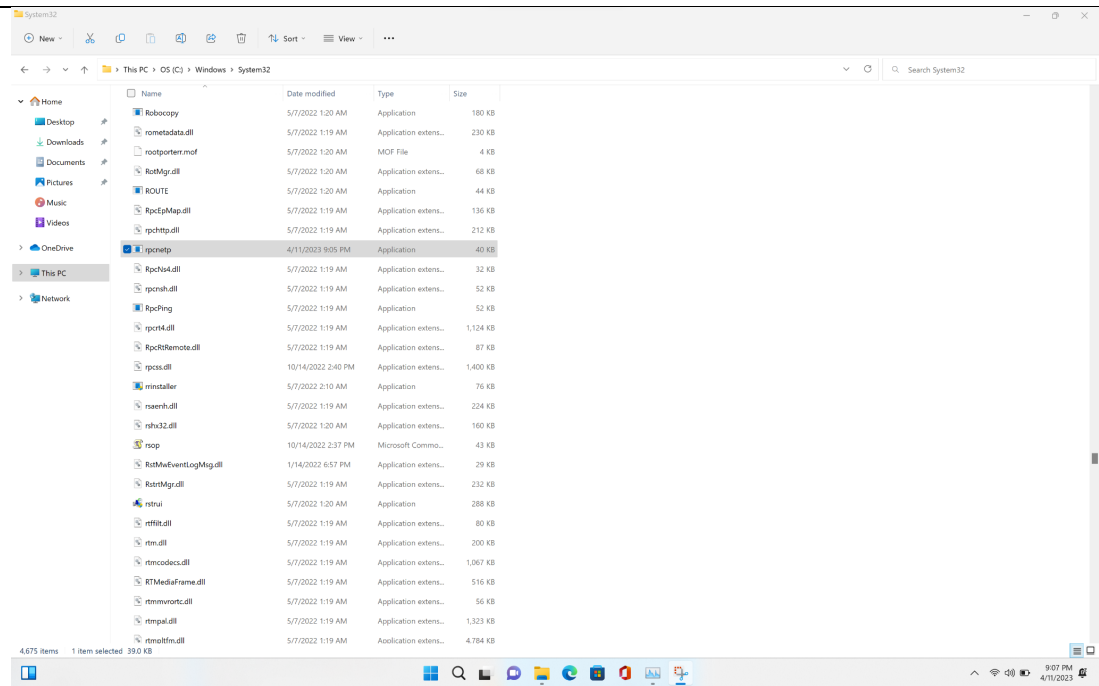
rpcnetp restarting process

The rpcnetp service then restarts the rpcnet process, which is one example of how the application component communicates with rpcnetp.

Name	Status	10% CPU	38% Memory	12% Disk	1% Network
Intel(R) Dynamic Application Loader Host Interface		0%	1.0 MB	0 MB/s	0 MBps
Intel(R) Innovation Platform Framework Service		0%	1.4 MB	0 MB/s	0 MBps
Intel(R) Innovation Platform Framework Service Container		0%	2.1 MB	0 MB/s	0 MBps
Intel(R) Innovation Platform Framework Utility Application		0%	1.1 MB	0 MB/s	0 MBps
Intel(R) Management Engine WMI Provider Registration (32 bit)		0%	1.9 MB	0 MB/s	0 MBps
Intel(R) Rapid Storage Technology Management Service		0%	1.7 MB	0 MB/s	0 MBps
Intel(R) Graphics Command Center Service		0%	15.4 MB	0 MB/s	0 MBps
IntelAudioService		0%	22.6 MB	0 MB/s	0 MBps
Killer Analytics Service		0%	2.2 MB	0.5 MB/s	0 MBps
Killer Network Service		0%	78.0 MB	0.1 MB/s	0 MBps
KillerAPS		0%	6.0 MB	0.1 MB/s	0 MBps
Microsoft (R) Aggregator Host		0%	1.6 MB	0 MB/s	0 MBps
Microsoft Edge (7)		0%	51.7 MB	0.1 MB/s	0 MBps
Microsoft Office Click-to-Run (SxS)		0%	11.6 MB	0 MB/s	0 MBps
Microsoft OneDrive		0%	11.7 MB	0.1 MB/s	0 MBps
Microsoft Teams (7)		2.1%	199.8 MB	4.6 MB/s	0 MBps
Microsoft Windows Search Indexer		0%	15.2 MB	0.9 MB/s	0 MBps
Microsoft® Volume Shadow Copy Service		0%	1.6 MB	0 MB/s	0 MBps
ModSG Core Worker Process		0%	4.9 MB	0 MB/s	0 MBps
PC-Dector Dell SupportAssist API		0%	93.9 MB	0 MB/s	0 MBps
Realtek HD Audio Universal Service		0%	3.4 MB	0 MB/s	0 MBps
Realtek HD Audio Universal Service		0%	3.7 MB	0 MB/s	0 MBps
Realtek HD Audio Universal Service		0%	4.1 MB	0 MB/s	0 MBps
rpcnetnp (32 bit)		0%	1.3 MB	0 MB/s	0 MBps
Runtime Broker		0%	1.2 MB	0 MB/s	0 MBps
Runtime Broker (2)		0%	1.6 MB	0 MB/s	0 MBps
SessionService		0%	0.5 MB	0 MB/s	0 MBps
Sink to receive asynchronous callbacks for WMI client application		0%	1.1 MB	0 MB/s	0 MBps
Spatial License AppService Broker		0%	1.8 MB	0 MB/s	0 MBps
Spooler Subsystem App		0%	4.3 MB	0.1 MB/s	0 MBps
Start (2)		0%	32.9 MB	0.1 MB/s	0 MBps
Touch Keyboard and Handwriting Panel		0%	2.4 MB	0 MB/s	0 MBps

rpcnetnp reinstalling rpcnet

Another example of the connection between these two components can be observed when rpcnetnp restores the rpcnet executable and .dll files when they were deleted. Both the rpcnet and rpcnetnp services can be terminated, as well as have both their files deleted.

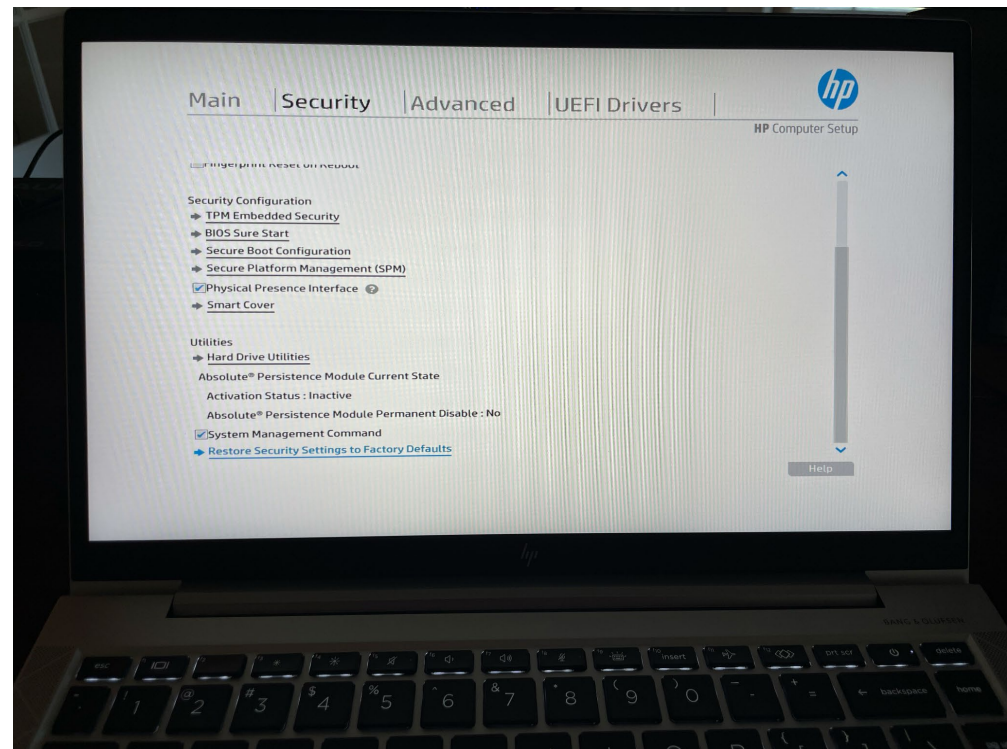


rpcnet reinstalled

The security service offered by Absolute exhibits the claim language of having the ability to communicate over a secure medium with a system server. Through the use of secure communication protocols (i.e., TLS) the system components can communicate with a remote server over a secure channel. The use of secure communication protocols, such as TLS and HTTPS, has become increasingly standard.

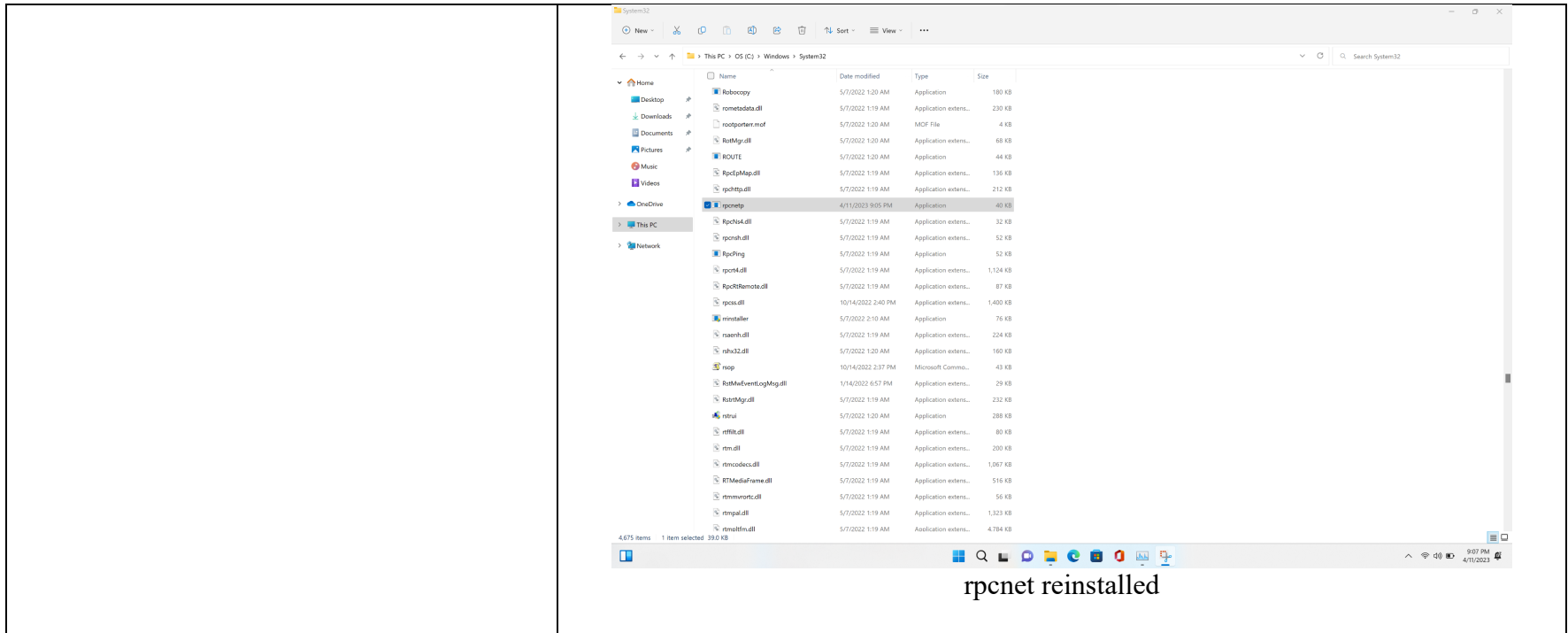
However, in the event that a secure channel is not directly pre-established, a secure medium can still be used via other means such as using a VPN that implements the WireGuard protocol. This is another scenario, in which the system components can communicate with a remote server over a secure channel.

The Absolute Backdoor Revisited explains how the bios component (i.e., rpcnetp BIOS agent and autochk.exe) are connected to rpcnetp (rpcnetp.exe windows service) through the bios component checking placing a new rpcnetp .dll file in windows on startup and spawning the rpcnetp.exe windows service for reinstalling and restarting rpcnet.exe. This is further validated with experimental analysis. It is seen that the Absolute bios component was indeed installed in the bios.



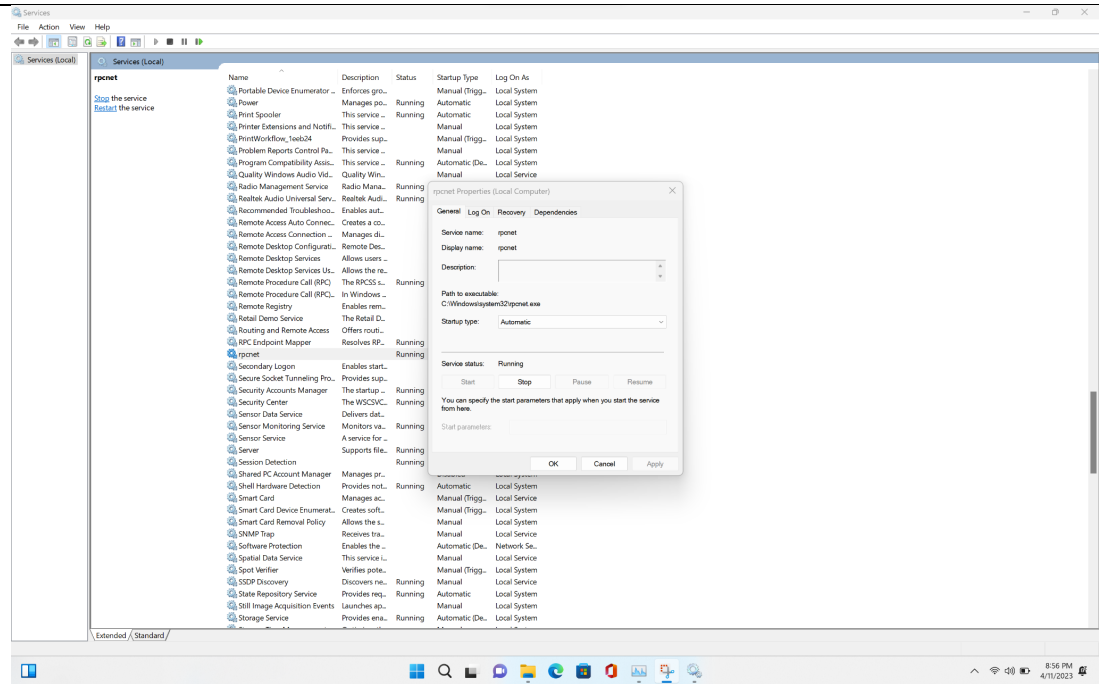
Application with BIOS settings of electronic device

Through observation of what occurs when the rpcnet and rpcnetp .dll files are deleted, it is apparent that the rpcnetp application file was restored automatically despite not existing on to the operating system. This is due to the BIOS restoring rpcnetp.



	<i>Chapter 1: Introduction</i> Absolute® brings a fundamentally new approach to cybersecurity by enabling self-healing endpoint security to ensure uncompromised visibility and near real-time remediation of breaches at the source. Our cloud-based platform and embedded Persistence technology puts IT and security professionals in control of devices, data, and applications — whether they are on or off the network — to improve IT asset management, ensure compliance, protect data, and reduce insider threats. Patented Persistence technology is embedded in the firmware of more than 1 billion popular PC and mobile devices from global manufacturers including Acer, Asus, Dell, Fujitsu, HP, Intel, Lenovo, Microsoft, Panasonic, Samsung and Toshiba. Absolute is an adaptive endpoint security solution. Its technology platform is a client/server architecture that delivers device security, data security, and asset management of endpoints, even if a device is off the network or in the hands of an unauthorized user. The persistent connection between the secure and patented agent (client) and the Absolute Monitoring Center (server) ensures organizations have protected access to up-to-date information about their entire device inventory. Authorized users can use the built-in tools in the Absolute console to track devices and initiate data and device security operations for the purposes of enforcing compliance policies, identifying at-risk computers, and taking preemptive and reactive measures if a security incident occurs. https://help.absolute.com/corporate/html5/en/Content/PDFs/EN/AbsoluteUG.en.pdf
[1m] wherein the security application receives the notification from at least one of the servers via the system area.	The Accused Instrumentalities comprise “wherein the security application receives the notification from at least one of the servers via the system area.” On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element. The entire application agent [security application] resides in a system area and therefore the security application receives the notification from at least one of the servers via the system area. Such communication is encrypted so as not to be decipherable outside of the system area.

	What type of protection is provided for communication between the Absolute agent and the Absolute Monitoring Center? The communication between the software agent and the Absolute Monitoring Center is encrypted. Optionally, you can also enable FIPS-140 certified communication. The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. The National Institutes of Standards and Technology (NIST) publishes the list of vendors with validated FIPS 140-1 and 140-2 cryptographic modules. The Absolute Encryption Engine is validated FIPS 140-2 and the certificate can be viewed here: Certificate 1680. https://www.absolute.com/media/2467/faq-absolute-persistence-absolute-software.pdf Analysis of the Absolute software and web interface confirms aspects of the infringing functionality. This is supported by V. Kamlyuk, S. Belov and A. Sacco, “Absolute Backdoor Revisited,” BlackHat, June 2014. [Online]. Available: https://www.blackhat.com/docs/us-14/materials/us-14-Kamluk-Computrace-Backdoor-Revisited-WP.pdf (last accessed April 27, 2023) (hereafter “Absolute Backdoor Revisited”). Absolute Backdoor Revisited, which is further confirmed with analysis of Absolute’s software. After locating the rpcnet.exe windows service, its execution can be terminated. This would then disable the absolute software from maintaining a connection with the servers.
--	---



rpcnet windows service Image

Once the process is terminated, the rpcnetp service begins execution in order to download and reinstall the rpcnetp service from the server.

Name	Status	CPU	Memory	Private	Network
Microsoft® Volume Shadow Copy Service		0%	1.2 MB	0 MB/s	0 Mbps
PC Doctor Dell SupportAssist API		0%	86.8 MB	0 MB/s	0 Mbps
Realtek HD Audio Universal Service		0%	2.5 MB	0 MB/s	0 Mbps
Realtek HD Audio Universal Service		0%	2.5 MB	0 MB/s	0 Mbps
Realtek HD Audio Universal Service		0%	3.3 MB	0 MB/s	0 Mbps
rpcnetp (32 bit)		0%	1.3 MB	0 MB/s	0 Mbps
rpcnetp		0%	1.1 MB	0 MB/s	0 Mbps
Runtime Broker		0%	1.0 MB	0 MB/s	0 Mbps
Runtime Broker		0%	0.4 MB	0 MB/s	0 Mbps
SessionService		0%	0.7 MB	0 MB/s	0 Mbps
Sink to receive asynchronous callbacks for WMI client application		0%	3.7 MB	0 MB/s	0 Mbps
Spooler SubSystem App		0.1%	31.8 MB	0.1 MB/s	0 Mbps
Start (2)		0.8%	2.7 MB	0.1 MB/s	0.1 Mbps
svchost.exe		0%	2.0 MB	0 MB/s	0 Mbps
Touch Keyboard and Handwriting Panel		0%	1.5 MB	0 MB/s	0 Mbps
Usermode Font Driver Host		0%	1.3 MB	0 MB/s	0 Mbps
Usermode Font Driver Host		0%	2.4 MB	0 MB/s	0 Mbps
Waves Audio Service		0.1%	112.8 MB	0 MB/s	0 Mbps
WavesMaxAudio Service Application		0%	13.3 MB	0 MB/s	0 Mbps
WavesSysSvc Service Application		0.2%	152.4 MB	0.8 MB/s	0 Mbps
Widgets (7)		0%	1.6 MB	0 MB/s	0 Mbps
Windows Audio Device Graph Isolation		0%	1.0 MB	0 MB/s	0 Mbps
Windows Defender SmartScreen		0%	8.9 MB	0 MB/s	0 Mbps
Windows Driver Foundation - User-mode Driver Framework Host ...		0%	1.3 MB	0 MB/s	0 Mbps
Windows Driver Foundation - User-mode Driver Framework Host ...		0.2%	8.7 MB	0 MB/s	0 Mbps
Windows Driver Foundation - User-mode Driver Framework Host ...		0.8%	21.6 MB	1.5 MB/s	0.1 Mbps
Windows Input Experience (3)		0%	1.0 MB	0 MB/s	0 Mbps
Windows Modules Installer		0%	1.9 MB	0 MB/s	0 Mbps
Windows Security Health Service		0%	0.9 MB	0 MB/s	0 Mbps
Windows Security notification icon		0%	2.7 MB	0 MB/s	0 Mbps
Windows Service Wrapper		0%	0.9 MB	0 MB/s	0 Mbps
Windows Wireless LAN 802.11 Extensibility Framework					

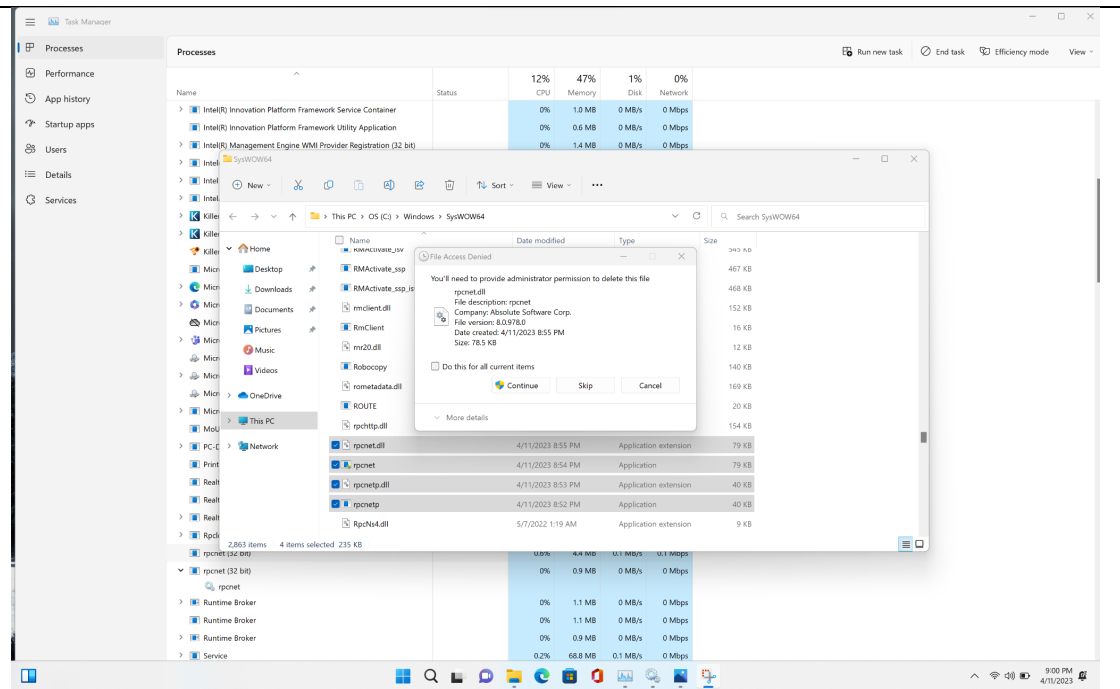
rpcnetp restarting process

The rpcnetp service then restarts the rpcnet process, which is one example of how the application component communicates with rpcnetp.

Name	Status	10% CPU	38% Memory	12% Disk	1% Network
Intel(R) Dynamic Application Loader Host Interface		0%	1.0 MB	0 MB/s	0 MBps
Intel(R) Innovation Platform Framework Service		0%	1.4 MB	0 MB/s	0 MBps
Intel(R) Innovation Platform Framework Service Container		0%	2.1 MB	0 MB/s	0 MBps
Intel(R) Innovation Platform Framework Utility Application		0%	1.1 MB	0 MB/s	0 MBps
Intel(R) Management Engine WMI Provider Registration (32 bit)		0%	1.9 MB	0 MB/s	0 MBps
Intel(R) Rapid Storage Technology Management Service		0%	1.7 MB	0 MB/s	0 MBps
Intel(R) Graphics Command Center Service		0%	15.4 MB	0 MB/s	0 MBps
IntelAudioService		0%	22.6 MB	0 MB/s	0 MBps
Killer Analytics Service		0%	2.2 MB	0.5 MB/s	0 MBps
Killer Network Service		0%	78.0 MB	0.1 MB/s	0 MBps
KillerAPS		0%	6.0 MB	0.1 MB/s	0 MBps
Microsoft (R) Aggregator Host		0%	1.6 MB	0 MB/s	0 MBps
Microsoft Edge (7)		0%	51.7 MB	0.1 MB/s	0 MBps
Microsoft Office Click-to-Run (SxS)		0%	11.6 MB	0 MB/s	0 MBps
Microsoft OneDrive		0%	11.7 MB	0.1 MB/s	0 MBps
Microsoft Teams (7)		2.1%	199.8 MB	4.6 MB/s	0 MBps
Microsoft Windows Search Indexer		0%	15.2 MB	0.9 MB/s	0 MBps
Microsoft® Volume Shadow Copy Service		0%	1.6 MB	0 MB/s	0 MBps
ModSG Core Worker Process		0%	4.9 MB	0 MB/s	0 MBps
PC-Dector Dell SupportAssist API		0%	93.9 MB	0 MB/s	0 MBps
Realtek HD Audio Universal Service		0%	3.4 MB	0 MB/s	0 MBps
Realtek HD Audio Universal Service		0%	3.7 MB	0 MB/s	0 MBps
Realtek HD Audio Universal Service		0%	4.1 MB	0 MB/s	0 MBps
rpcnetp (32 bit)		0%	1.3 MB	0 MB/s	0 MBps
Runtime Broker		0%	1.2 MB	0 MB/s	0 MBps
Runtime Broker (2)		0%	1.6 MB	0 MB/s	0 MBps
SessionService		0%	0.5 MB	0 MB/s	0 MBps
Sink to receive asynchronous callbacks for WMI client application		0%	1.1 MB	0 MB/s	0 MBps
Spatial License AppService Broker		0%	1.8 MB	0 MB/s	0 MBps
Spooler Subsystem App		0%	4.3 MB	0.1 MB/s	0 MBps
Start (2)		0%	32.9 MB	0.1 MB/s	0 MBps
Touch Keyboard and Handwriting Panel		0%	2.4 MB	0 MB/s	0 MBps

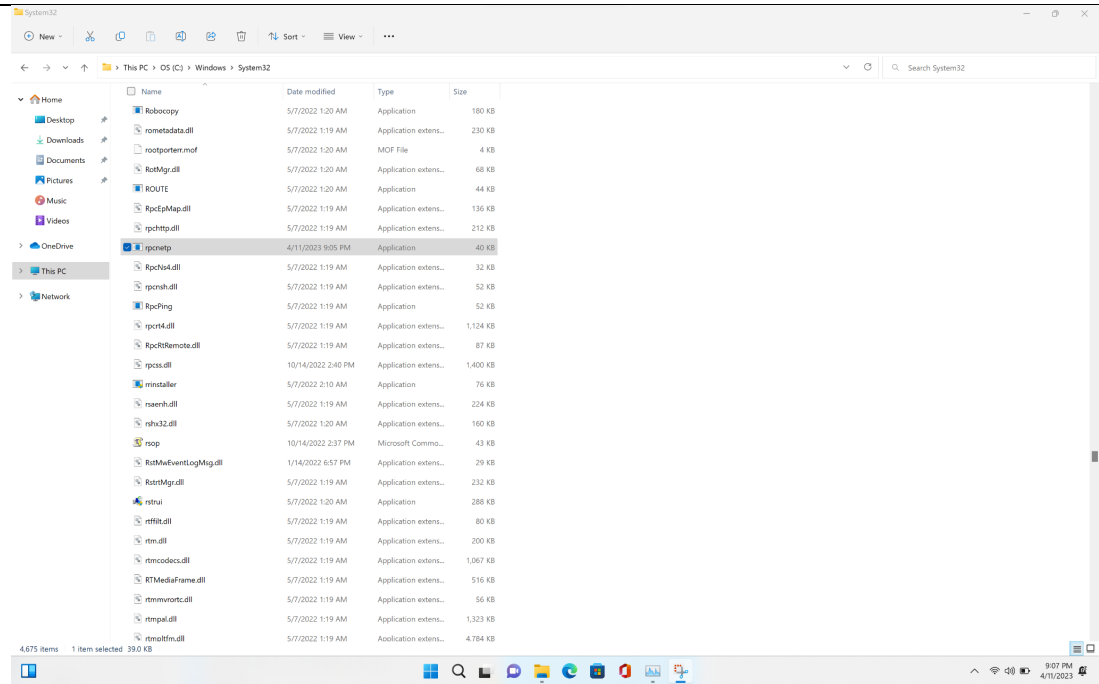
rpcnetp reinstalling rpcnet

Another example of the connection between these two components can be observed when rpcnetp restores the rpcnet executable and .dll files when they were deleted. Both the rpcnet and rpcnetp services can be terminated, as well as have both their files deleted.



.dll files being deleted

As was expected and supported by **Absolute Backdoor Revisited**, The BIOS component restores the rpcnetp windows service. After restoration, the rpcnetp service is executed which restores rpcnet, via downloading the rpcnet files from the remote server and reinstalling.

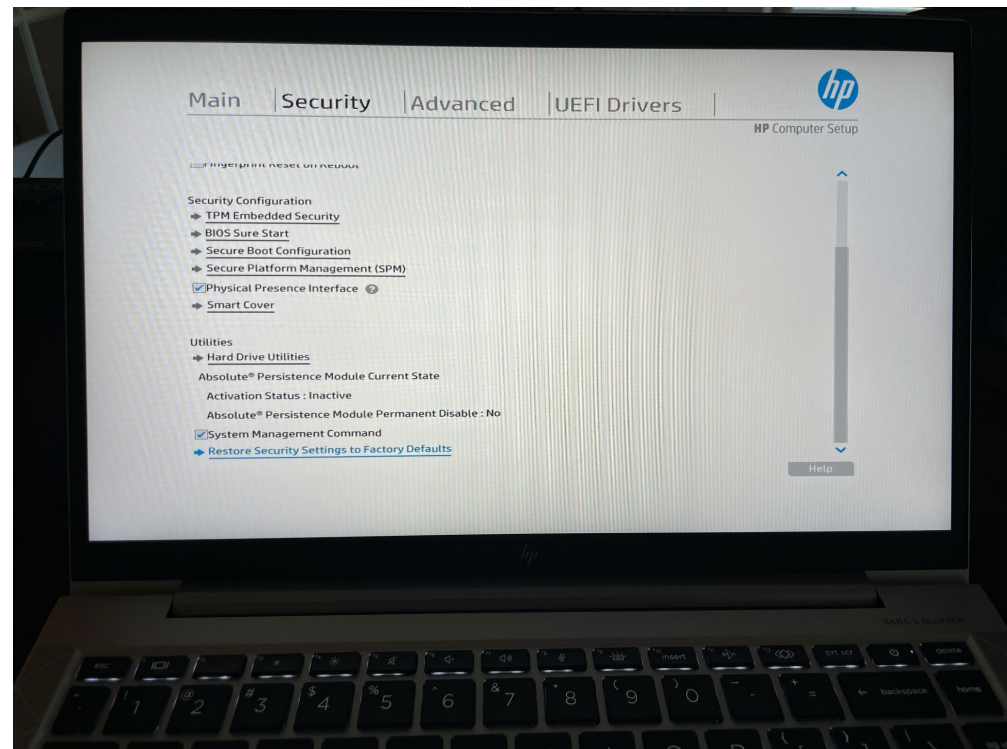


rpcnet reinstalled

The security service offered by Absolute exhibits the claim language of having the ability to communicate over a secure medium with a system server. Through the use of secure communication protocols (i.e., TLS) the system components can communicate with a remote server over a secure channel. The use of secure communication protocols, such as TLS and HTTPS, has become increasingly standard.

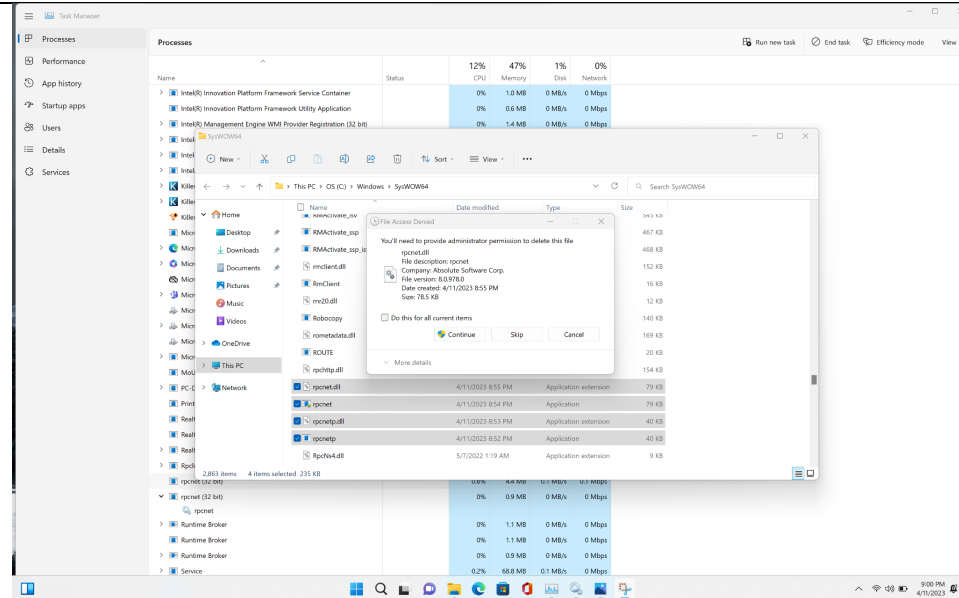
However, in the event that a secure channel is not directly pre-established, a secure medium can still be used via other means such as using a VPN that implements the WireGuard protocol. This is another scenario, in which the system components can communicate with a remote server over a secure channel.

The Absolute Backdoor Revisited explains how the bios component (i.e., rpcnetp BIOS agent and autochk.exe) are connected to rpcnetp (rpcnetp.exe windows service) through the bios component checking placing a new rpcnetp .dll file in windows on startup and spawning the rpcnetp.exe windows service for reinstalling and restarting rpcnet.exe. This is further validated with experimental analysis. It is seen that the Absolute bios component was indeed installed in the bios.



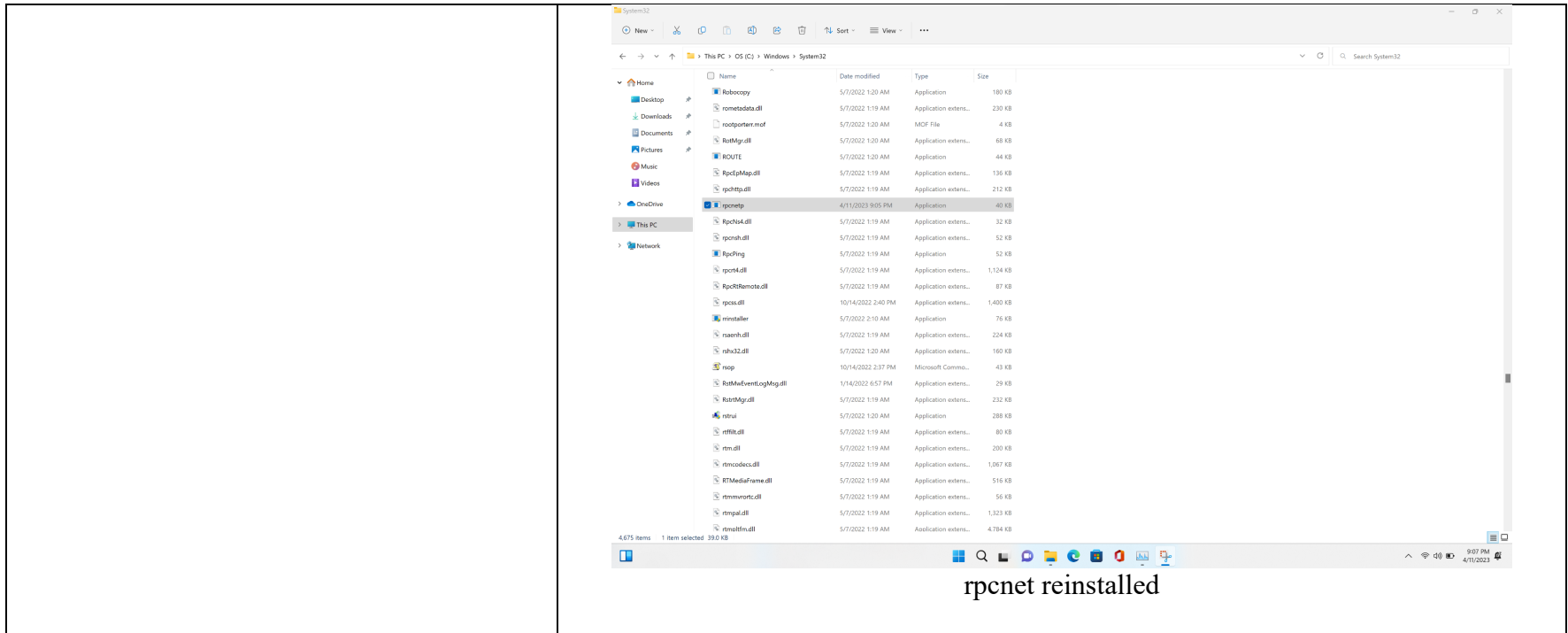
Application with BIOS settings of electronic device

Through observation of what occurs when the rpcnet and rpcnetp .dll files are deleted, it is apparent that the rpcnetp application file was restored automatically despite not existing on to the operating system. This is due to the BIOS restoring rpcnetp.



.dll files being deleted

After being restored, the files can be seen again in the windows operating system.



Chapter 1: Introduction

Absolute® brings a fundamentally new approach to cybersecurity by enabling self-healing endpoint security to ensure uncompromised visibility and near real-time remediation of breaches at the source. Our cloud-based platform and embedded Persistence technology puts IT and security professionals in control of devices, data, and applications — whether they are on or off the network — to improve IT asset management, ensure compliance, protect data, and reduce insider threats. Patented Persistence technology is embedded in the firmware of more than 1 billion popular PC and mobile devices from global manufacturers including Acer, Asus, Dell, Fujitsu, HP, Intel, Lenovo, Microsoft, Panasonic, Samsung and Toshiba.

Absolute is an adaptive endpoint security solution. Its technology platform is a client/server architecture that delivers device security, data security, and asset management of endpoints, even if a device is off the network or in the hands of an unauthorized user.

The persistent connection between the secure and patented agent (client) and the Absolute Monitoring Center (server) ensures organizations have protected access to up-to-date information about their entire device inventory. Authorized users can use the built-in tools in the Absolute console to track devices and initiate data and device security operations for the purposes of enforcing compliance policies, identifying at-risk computers, and taking preemptive and reactive measures if a security incident occurs.

<https://help.absolute.com/corporate/html5/en/Content/PDFs/EN/AbsoluteUG.en.pdf>

For example, **Absolute Backdoor Revisited** shows that the BIOS component is configured to determine whether rpcnetp is present and whether rpcnetp has been tampered with.

Absolute Backdoor Revisited explains how Absolute's security service possesses a BIOS security component (autochk.exe and the rpcnetp BIOS module) determines whether the integrity of the application component during a boot process for the electronic device. During the boot process the autochk.exe returns the local file rpcnetp.exe and changes the local system registry to create a new system service called rpcnetp. The purpose of this is to check the integrity during the boot process of the rpcnetp windows service and can inject a freshly created rpcnetp.dll into its memory.

Stage 1: BIOS module

The first stage (after main BIOS initialization) is to execute modules from Option ROM. At this point the Computrace code searches for available disk drives and analyzes the partition table. If FAT/FAT32/NTFS partitions are found, it locates the Windows installation path and autochk.exe application. Next, it creates a backup of system default autochk.exe code parts and overwrites them with its own code. These parts are saved as autochk.exe.bak file on FAT or autochk.exe:BAK NTFS ADS stream on NTFS filesystem. This can be used as an indicator of Computrace activity at stage one.

On some systems where the Computrace module is not part of the BIOS or it cannot be activated, a different approach is used. On such systems the Computrace activation code modifies the MBR of the hard drive and takes control of the PC at the earliest stage of the system boot. Apparently this approach is not as persistent as a BIOS-based dropper.

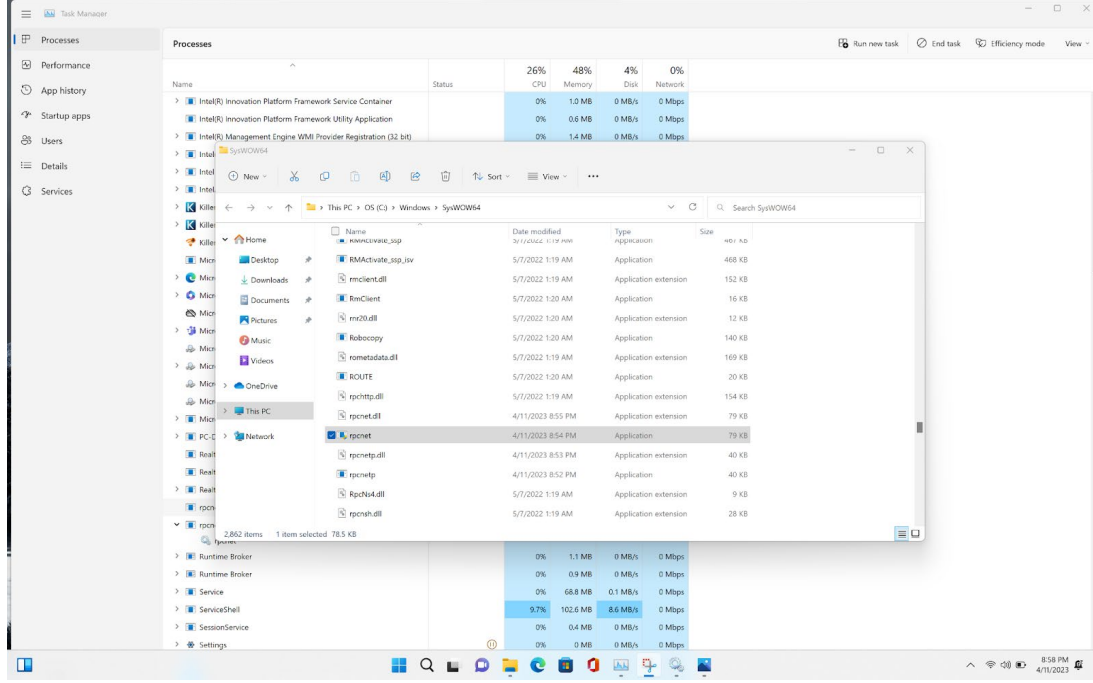
Stage 2: autochk.exe

At this stage a modified autochk.exe starts and has full access to the local file system as well as system registry via Windows NT Native API calls. Its main purpose is to drop the local file rpcnetp.exe and change the local system registry to create a new system service called rpcnetp. The original autochk.exe code is then restored.

BIOS execution process discussed in [Absolute Backdoor Revisited](#)

Testing confirms that the Accused Instrumentalities include that the BIOS component is configured to determine whether rpcnetp is present and whether rpcnetp has been tampered with.

Through observing the rpcnetp windows service files on the computer after the Absolute software is installed, an examination of the file creation times indicates they were created during the boot process.

	 The screenshot shows the Windows Task Manager 'Processes' tab with a list of running processes. Below it, a File Explorer window is open to the 'SysWOW64' directory, displaying a list of files including 'rpcnetp.dll'. The file is highlighted, indicating it is the target of an action. rpcnetp.dll file Moreover, the same can be observed for when the .dll files for rpcnetp are deleted and restored by the BIOS during a subsequent boot
7. A mobile electronic device according to claim 1, wherein the operations the security application is operable to perform further comprise: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.	The Accused Instrumentalities include a mobile electronic device after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device. On information and belief, review of Absolute’s source code review will further demonstrate that the Accused Instrumentalities perform this claim element.

	I am concerned about privacy issues. What kind of information do you collect from my computer? Standard communication between your computer and our Monitoring Center occurs once a day and consists of basic information like memory size, hard drive size, type of processor, type of operating system, user name, IP and Mac addresses. There is no active monitoring of your computer until you report a theft. After a theft is reported, your computer will contact our Monitoring Center every 15 minutes. This increased contact allows the Absolute Theft Recovery Team to obtain specific details about where your computer is located, who is using it, and what they're doing with it. LFL FAQ at 4.
--	---

Classic File List and File Retrieval:

We are in the process of retiring the Classic File List and File Retrieval features across all customers. Certain customers can still access the features through the 'File List Summary Report' and 'File Retrieval Summary Report' respectively under the 'Settings' pane of the console. Both reports will be completely retired across all customers on March 4th. Going forward, please utilize the following four Absolute Reach scripts as replacements for the retired Classic features:

Replacing the Classic File Retrieval feature:

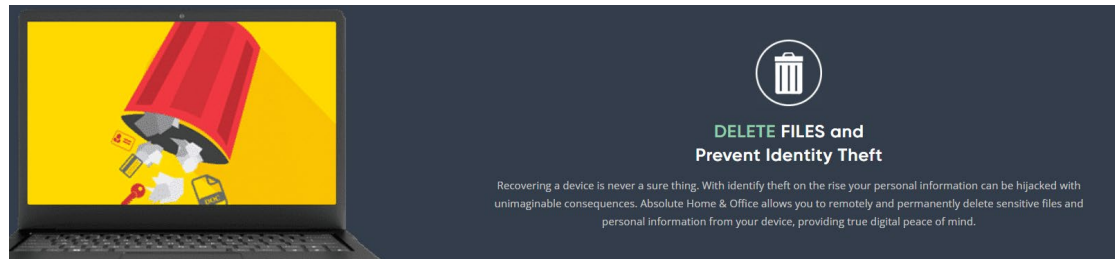
- Upload files to Dropbox
- Upload files to FTP server
- Upload files to network shared folder

<https://community.absolute.com/s/article/Product-Update-End-of-Life-of-Classic-Absolute-Features>

Vancouver, Canada: December 7, 2010 – **Absolute® Software Corporation** (“Absolute” or the “Company”) (TSX: ABT), the leading provider of firmware-based, patented, computer theft recovery, data protection and secure computer lifecycle management solutions announced today that its SaaS computer tracking solution Computrace® now includes Remote File Retrieval. With this new data leakage prevention (DLP) feature, IT administrators can use the Computrace cloud to identify and retrieve sensitive company files that are exposed on end point devices. This can be done proactively to mitigate the risk of data loss, or as an emergency response action on missing or stolen devices prior to remotely wiping the hard drive for complete corporate data security.

In addition to being an exciting new security feature in Computrace, the Remote File Retrieval (RFR) feature can be an essential productivity tool. For example, a travelling executive works on a confidential PowerPoint presentation on the plane, but leaves her laptop in a cab on the way to her hotel. Once notified, IT may be able to remotely retrieve the lost file and send it to the executive in time for her partner meetings.

<https://www.absolute.com/company/press-releases/2010/absolute-empowers-it-with-new-data-leakage-prevention-capabilities/>



<https://homeoffice.absolute.com/features/>

Remotely Delete Data From Devices

^ Selectively delete files

OS Support:  

<https://www.absolute.com/platform/compare-absolute-products/>

	Deleting Files on Your Device You may have very private and sensitive data on your device that is more important to you than the device. In case of theft or loss, you can remotely delete some or all files on your device using our Data Delete technology. When you delete a file, your device does not actually remove the contents of the file. Instead, the device simply unlinks the file from the file directory system, leaving the contents of the file in the disk sectors. Data from the file remains until the operating system re-uses the same sectors when writing new data. Until the old data is overwritten (which may take months or even longer), data can be recovered by programs that read disk sectors directly. Using our advanced technology, you can eliminate all data associated with a file you want to delete. https://help.absolute.com/html5/en/Content/New%20Consumer%20Web%20Help/Section_3/Deleting/DeletingFiles.htm
[9pre] A method for providing security for a mobile electronic device, the method comprising:	The Accused Instrumentalities practice this claim element. <i>See</i> citations and analysis for claim 1 and the remaining elements of claim 9.
[9a] receiving, at a mobile electronic device, a request from an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers;	The Accused Instrumentalities practice this claim element. <i>See</i> citations and analysis for claim element 1d.
[9b] in response to the request from the owner, registering the mobile electronic device with the security service;	The Accused Instrumentalities practice this claim element. <i>See</i> citations and analysis for claim element 1d, 1f.
[9c] automatically sending identifying information for the mobile electronic device from the mobile electronic device to the security service;	The Accused Instrumentalities practice this claim element. <i>See</i> citations and analysis for claim element 1e.

[9d] after the owner has registered the mobile electronic device with the security service, periodically communicating with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1f.
[9e] after the owner has registered the mobile electronic device with the security service, accepting a notification from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device;	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1g.
[9f] in response to accepting the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1h.
[9g] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1i.
[9h] wherein the mobile electronic device comprises non-volatile memory;	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1j.
[9i] wherein the non-volatile memory comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user;	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1k.
[9j] wherein the security application utilizes code residing at least partially in the system area; and	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1l.
[9k] wherein the operation of accepting the notification from the security service	The Accused Instrumentalities practice this claim element. See citations and analysis for claim element 1m.

comprises receiving the notification from at least one of the servers via the system area.	
15. A method according to claim 9, further comprising: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.	The Accused Instrumentalities practice this claim element. <i>See</i> citations and analysis for claim 7.