



- [Engineering](#)
- [Become a Partner](#)
- [Contact Us](#)
- [Client Login](#)



- [Services](#)
 - - DETECT AND RESPONSE
 - [Managed Detection & Response \(MDR\)](#)
 - [Managed Endpoint Detection & Response \(EDR\)](#)
 - [Digital Risk and Threat Monitoring](#)
 - [Managed Endpoint Protection \(EPP\)](#)
 - [Decoy & Deception Honeypots Service](#)
 - [Managed Network Detection & Response \(Powered by Darktrace\)](#)
 - [Managed Azure Sentinel – Detection & Response](#)
 - MANAGE AND AUDIT
 - [Managed Firewall](#)
 - [Vulnerability Management Service](#)
 - [ISO 27001 & Security Compliance](#)
 - [Penetration Testing Service](#)
 - [CISO as a Service](#)
 - [Web Application Security Testing](#)
 - [Managed Data Security \(Powered by IBM Security Guardium\)](#)



[datasheets](#)

[Managed Azure Sentinel - Detection & Response](#)

[Download datasheet →](#)

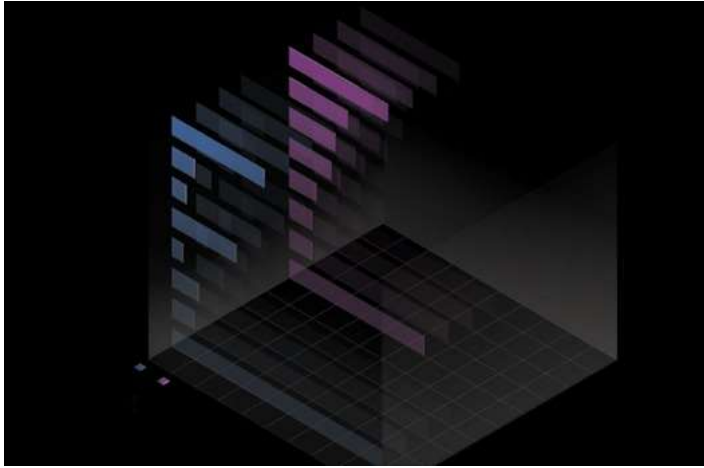


[Request 30-Day MDR Free Proof of Value](#)

[Request POV →](#)

- [Our Platform](#)
- [Industries](#)
 - - [All Industries](#)
 - [Public Sector](#)
 - [Education](#)
 - [Finance](#)
 - [Healthcare](#)
 - [Telecommunications](#)
 - [Transport](#)
 - [Energy](#)
 - [Manufacturing](#)
 - [Property & Construction](#)
 - [Retail](#)
 - [Legal](#)
 - [Media](#)
 - [Technology](#)

FEATURED CONTENT



reports

[IBM X-Force Threat Intelligence Index 2021](#)

[Download report →](#)



[Request a Free Managed Firewall Audit](#)

[Request POV →](#)

- [Knowledge Base](#)
 - [Datasheets](#)
 - [Webinars](#)
 - [White Papers](#)
 - [Reports](#)
 - [Videos](#)
 - [Events](#)
 - [Press Releases](#)

FEATURED CONTENT



whitepapers

[The Early Indications of a Breach. Cyber Kill Chain Analysis. Part 2 of 2.](#)

[Download white paper](#)



whitepapers

[Machine Learning for Ransomware Detection, Cyber Kill Chain Analysis, Part 1 of 2](#)

[Download white paper](#)

- [Blog](#)
 - [Company](#)
 - [About Us](#)
 - [Careers](#)
 - [Meet Our Team](#)
- FROM THE BLOG



[SecurityHQ Investigates HAENIUM Exchange Server Compromise](#)

[Read more](#)



[Why the Education Sector Needs to Make Cyber Security a Priority](#)

[Read more](#)

[VIEW ALL](#)

- [TRIALS](#)

-

FEATURED TRIALS



[Free Managed Firewall Audit](#)

[REQUEST FREE AUDIT](#)



[Request 30-Day MDR Free Proof of Value](#)

[REQUEST FREE POV TRIAL](#)

[VIEW ALL](#)

Notes from the Field • 15 MIN READ

Notes from the Field. Using Proxy Logs to Detect Suspicious Activity – Interview with Aaron Hambleton.

by Eleanor Barlow • Jan 2021

- -

The job of a Proxy is to provide a gateway between the users and the internet. A good quality, well configured Proxy assists in keeping users and the internal network protected from the nefarious content published and accessible on the internet.

[‘If you’re like most people, you probably associate proxy servers with unblocking Netflix content from other countries or staying a bit more secure on an open WiFi network. The reality, however, is that proxy servers do much more — and are especially vital for businesses.’](#) – RJ Prego (CMSWire)

All network traffic flowing out of the network should be passing through a Proxy, and the logs typically provide a rich repository of meta data. This inherently makes Proxy logs a great resource for [Threat Hunting](#).

What Data Can Proxy Logs Give You?

Proxy logs contain a lot of valuable data which can be used for detecting suspicious activity. Listed below are some examples of what data can be extracted from the logs, and this list is just the start.

Destination Host Name	The domain or URL being accessed
Destination IP	The IP address being accessed
Destination Port	The network port being accessed
User Agent	The User Agent used to initiate the traffic (Chrome, Mozilla, Curl)
Request Method	Was it a GET or POST request?
Device Action	Did the proxy allow or deny the requested traffic?
Referrer	Who referred the traffic towards the Destination Host Name?
Domain/URL Category	What is the Domain/URL categorised as? (i.e., Malicious or Business)
Requested File Name	The requested file name when accessing a website

Detecting Suspicious Network Traffic with Proxy Logs. Real-Life Example

SecurityHQ’s team of security experts [routinely hunt](#) for suspicious and potentially malicious activity in our customer networks. During a recent investigation, [Aaron Hambleton](#), one of SecurityHQ’s Security Monitoring and Incident Response Leads, identified an unapproved third-party management application installed on a Domain Controller routinely beaconing to a suspicious URL.

Aaron leads a 24/7 Security Operation Centre in the Middle East. With 10+ years of experience in cyber security, he has worked in Financial Services, Retail, Insurance, Government, and Telecommunication industries as a security consultant and incident response analyst.

Aaron is a GIAC certified Defence Analyst with extensive knowledge in Security Blue Teaming, Incident Response, Cyber Security Operations, Cloud Security, and Cyber Security consultancy in an advisory capacity.

Aaron, can you provide some context and analysis of what happened in this example?

Aaron: “Well, to start the analysis, I extracted the proxy logs from SIEM. For me, raw data is much easier to manipulate and pivot with. Once I had the logs I wanted to check for any anomalies like strange User Agents, request methods, and potentially suspicious file download requests.

I will typically focus on the least common events first and then pivot when I find something interesting.

In this case, I observed that a single Domain Controller was having frequent outbound connections to a suspicious URL with a PowerShell UserAgent. This isn’t normal behaviour and given the criticality of the server and the fact that this behaviour was observed on no other servers, I decided to dig further.

Here you can see the detected Powershell UserAgent initiating the outbound network traffic.”

What did you do next?

Aaron: “Next, I focused on the Domain Controller itself. I wanted to get an idea of what was happening on this server. Using an [Endpoint Detection & Response](#) (EDR) tool I was able to analyse all PowerShell processes on the Domain Controller which were having outbound network connections towards the IP identified in the Proxy logs. My analysis revealed that PowerShell was being used to call and execute a script in order to initiate the connection.”

The command line parameters for script execution are shown below. (Sections in black redacted for confidentiality).

What did you do with this information?

Aaron: “Once I had identified the script being used to initiate the outbound connections, I was able to download a copy of it from the server and review the code contained inside. Reviewing scripts and code is an important step in investigating suspicious activity, it really helps as an analyst to understand what a script is attempting to execute”

Below is a code snippet taken from the script

For those less proficient in coding, what is noticeable about this?

Aaron: “After reviewing the script, I noticed that there was a URL defined in a variable named \$WebCheck. The URL contains a path to a .txt file. When the script executes, it uses the Invoke-WebRequest PowerShell ‘cmdlet’ to download the file from the URL defined in the \$WebCheck variable.

In this particular case, it transpired that I had discovered a third-party administration tool on a Domain Controller which was not part of the organisations approved software list. We often refer to these tools as a Potentially Unwanted Program or PUP for short.

Adversaries have previously demonstrated that they will target third party administration and management tools. In this example there was a real risk that the genuine file being downloaded by the script could have been replaced with a malicious binary or script, paving the way for a potentially devastating attack.”

Why are these called ‘Potentially Unwanted Program’? Surely, elements that flag up as potentially unwanted are all either unwanted or malicious?

Aaron: “Good question. Potentially Unwanted Programs (PUPs) are not malware. ‘[The main difference is that you give consent to download the PUP, even though you might not know about it if you didn’t read the agreements or installation process thoroughly.](#)’ (McAfee)

Some PUPs can contain spyware including keyloggers, and other software to gather your information. Even if the PUP doesn’t have any malicious content, they can slow down a device by consuming disk space on a device and it can weaken a device’s security, making it more vulnerable to malware.”

What do you suggest to organizations wanting to avoid such an event?

Aaron: “Having strict controls in place surrounding software installation on endpoints and servers is the first step in preventing these unwanted applications making their way into an organisation. There are a few basic steps an organisation can take to prevent this:

1. Use AppLocker or a similar product to stop unauthorized applications running within the environment. With AppLocker you can create rules to allow or deny applications from running based on unique identities of files and to specify which users or groups can run those applications.
2. Restrict the permissions of users to prevent them installing software without following the correct process.
3. Ensure that you have comprehensive endpoint security [software which can detect](#) PUPs and remove them remotely.

Thank you, Aaron.

If you have a question or would like to try our Managed Detection and Response service for 30-days at no cost, [contact us here](#).

•

LATEST STORIES

- [SecurityHQ Investigates HAFNIUM Compromise of Microsoft Exchange Servers – 10 March 2021](#)
Mar 2021
- [Why the Education Sector Needs to Make Cyber Security a Priority](#)
Mar 2021
- [Rising Security Concerns in the Telecom Industry](#)
Feb 2021
- [Cyber Security Talent – A Critical National Priority](#)
Jan 2021

•

CATEGORIES

- [Awards](#)
- [Business Culture](#)
- [Cybersecurity](#)
- [Industry Insights](#)
- [Industry News](#)
- [Notes from the Field](#)
- [SecurityHQ Update](#)

•

SIGN UP FOR OUR NEWSLETTER

First name*

Last name*

Email*

- ☐ Yes, I agree to receive periodic emails from SecurityHQ related to products and services and can unsubscribe at any time. I accept SecurityHQ's [private policy](#).*

SecurityHQ (a brand name of Si Consult Limited) 2021. All rights reserved.

Company

- [About us](#)
- [Meet our team](#)
- [Careers](#)
- [Blog](#)

Knowledge Base

- [Datasheets](#)
- [Videos](#)
- [Webinars](#)
- [White Papers](#)
- [Reports](#)
- [Events](#)
- [Press Releases](#)

Services

- [Managed Detection and Response \(MDR\)](#)
- [Managed Endpoint Detection & Response \(EDR\)](#)
- [Managed Firewall](#)
- [Digital Risk and Threat Monitoring](#)
- [Vulnerability Management Service](#)
- [Managed Endpoint Protection \(EPP\)](#)
- [Decoy & Deception Honeypots Service](#)
- [ISO 27001 & Security Compliance](#)
- [Penetration Testing Service](#)
- [Managed Network Detection & Response \(Powered by Darktrace\)](#)
- [CISO as a Service](#)
- [Web Application Security Testing](#)
- [Managed Data Security \(Powered by IBM Security Guardium\)](#)
- [Managed Azure Sentinel – Detection & Response](#)

Industries

- [Public Sector](#)
- [Education](#)
- [Finance](#)
- [Healthcare](#)
- [Telecommunications](#)
- [Transport](#)
- [Energy](#)
- [Manufacturing](#)
- [Property & Construction](#)
- [Retail](#)
- [Legal](#)
- [Media](#)
- [Technology](#)

[Platform](#)

- [Company](#)
- [About us](#)
- [Meet our team](#)
- [Careers](#)
- [Blog](#)

• [Our Platform](#)

- [Knowledge Base](#)
- [Datasheets](#)
- [Videos](#)
- [Webinars](#)
- [White Papers](#)
- [Reports](#)
- [Events](#)
- [Press Releases](#)

- [Industries](#)
- [Public Sector](#)
- [Education](#)
- [Finance](#)
- [Healthcare](#)
- [Telecommunications](#)
- [Transport](#)
- [Energy](#)
- [Manufacturing](#)
- [Property & Construction](#)
- [Retail](#)
- [Legal](#)
- [Media](#)
- [Technology](#)

- [Services](#)
- [Managed Detection and Response \(MDR\)](#)
- [Managed Endpoint Detection & Response \(EDR\)](#)
- [Managed Firewall](#)
- [Digital Risk and Threat Monitoring](#)
- [Vulnerability Management Service](#)
- [Managed Endpoint Protection \(EPP\)](#)
- [Decoy & Deception Honeypots Service](#)
- [ISO 27001 & Security Compliance](#)
- [Penetration Testing Service](#)
- [Managed Network Detection & Response \(Powered by Darktrace\)](#)
- [CISO as a Service](#)
- [Web Application Security Testing](#)
- [Managed Data Security \(Powered by IBM Security Guardium\)](#)
- [Managed Azure Sentinel – Detection & Response](#)

-

SecurityHQ (a brand name of Si Consult Limited) 2021. All rights reserved.

[Privacy Policy](#)

HQ

- [Services](#)
 - [>>](#)
 - [Our Platform](#)
 - [Industries](#)
 - [>>](#)
 - [Knowledge Base](#)
 - [>>](#)
 - [Blog](#)
 - [Company](#)
 - [>>](#)
 - [Contact](#)
- [Engineering](#)
 - [Become a Partner](#)
 - [Contact Us](#)
 - [Login](#)

[FREE TRIAL](#)

- [All Services](#)
- DETECT AND RESPONSE
 - [Managed Detection & Response \(MDR\)](#)
 - [Managed Endpoint Detection & Response \(EDR\)](#)
 - [Digital Risk and Threat Monitoring](#)
 - [Managed Endpoint Protection \(EPP\)](#)
 - [Decoy & Deception Honeypots Service](#)
 - [Managed Network Detection & Response \(Powered by Darktrace\)](#)
 - [Managed Azure Sentinel – Detection & Response](#)
- MANAGE AND AUDIT
 - [Managed Firewall](#)
 - [Vulnerability Management Service](#)
 - [ISO 27001 & Security Compliance](#)
 - [Penetration Testing Service](#)
 - [CISO as a Service](#)
 - [Web Application Security Testing](#)
 - [Managed Data Security \(Powered by IBM Security Guardium\)](#)

FEATURED CONTENT



datasheets

[Managed Azure Sentinel - Detection & Response](#)

[Download datasheet](#)



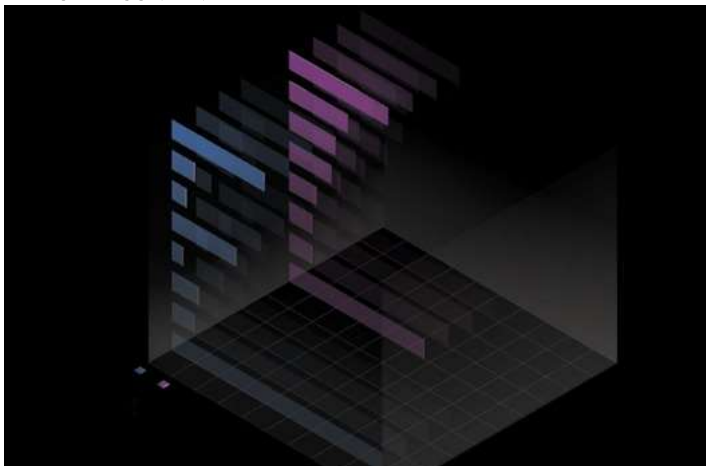
[Request 30-Day MDR Free Proof of Value](#)

[Request POV](#)

- [All Industries](#)
- [Public Sector](#)
- [Education](#)
- [Finance](#)
- [Healthcare](#)

- [Telecommunications](#)
- [Transport](#)
- [Energy](#)
- [Manufacturing](#)
- [Property & Construction](#)
- [Retail](#)
- [Legal](#)
- [Media](#)
- [Technology](#)

FEATURED CONTENT



reports

[IBM X-Force Threat Intelligence Index 2021](#)

[Download report](#)



[Request a Free Managed Firewall Audit](#)

[Request POV](#)

- [All Assets](#)
- [Datasheets](#)
- [Webinars](#)
- [Videos](#)
- [White Papers](#)
- [Reports](#)
- [Events](#)
- [Press Releases](#)

FEATURED CONTENT



whitepapers

[The Early Indications of a Breach. Cyber Kill Chain Analysis. Part 2 of 2.](#)

[Download white paper](#)



whitepapers

[Machine Learning for Ransomware Detection. Cyber Kill Chain Analysis. Part 1 of 2](#)

[Download white paper](#)

- [About Us](#)
- [Careers](#)
- [Meet Our Team](#)

FROM THE BLOG



[SecurityHQ Investigates HAFNIUM Exchange Server Compromise](#)

[Read more](#)



[Why the Education Sector Needs to Make Cyber Security a Priority](#)

[Read more](#)