

EXHIBIT 2028

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re <i>Ex Parte</i> Reexamination of	U.S. Patent No. 9,686,193
Control No.: 90/014,476	Group Art Unit: 3991
Filed: March 19, 2020	Confirmation No.: 1013
Patent Owner: Centripetal Networks, Inc.	Examiner: Minh T. Nguyen
For U.S. Patent No.: 9,686,193 – FILTERING NETWORK DATA TRANSFERS	

Submitted Electronically

Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

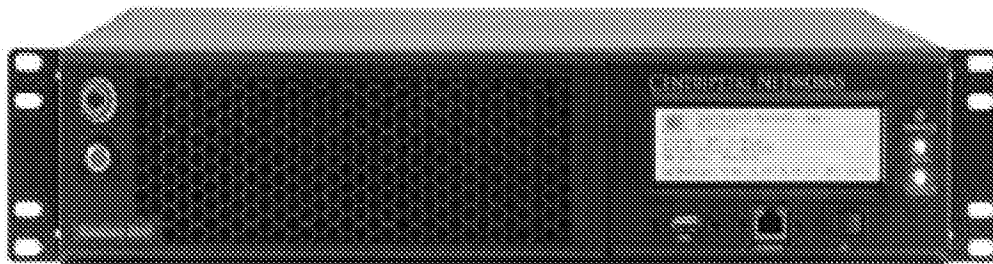
DECLARATION OF DR. SEAN MOORE
IN SUPPORT OF CENTRIPETAL'S RESPONSE TO NON-FINAL OFFICE ACTION

I, Sean Moore, Ph.D. declare:

1. I am over the age of 18 and make this declaration of my own personal knowledge.
2. Since 2010, I have been Chief Technology Officer (“CTO”) at Centripetal Networks, Inc. (“Centripetal”). Before joining Centripetal, I obtained a B.S. degree in Electrical Engineering in 1983, a M.S. degree in Mathematics in 1990, a M.S. degree in Computer Science in 1993, and a Ph.D. in Computer Science in 1994. Prior to starting at Centripetal, I also worked for sixteen (16) years at different companies developing new networking, communications, web and machine learning technologies, including at BBN Technologies.
3. I joined Centripetal (as its third employee) because I wanted to be part of a company whose intent and purpose was to solve the Internet cyber security problem once and for all. Our goal was to improve the security of the Internet via a new disruptive method and approach since existing approaches in the network security space were not working. In particular, Centripetal focuses on solving network security and network protection problems by “operationalizing” cyber threat intelligence (CTI). Our idea was to take cyber threat intelligence and somehow transform it so that it can be applied to live Internet traffic to secure the Internet, by essentially shutting down the cybercriminal communications and their attacks. The step of transforming raw CTI to operationalized CTI has been difficult. We had to develop new mathematics, new algorithms, and new technologies that could apply this operationalized CTI to live Internet traffic to stop cyber-attacks. In the end, Centripetal created a revolutionary network appliance marketed as RuleGATE™ (and other products) that is a CTI enforcement platform and threat intelligence gateway on which these operationalized CTI technologies are built.
4. As CTO, I lead Centripetal’s product development, research and development, and intellectual property protection. Centripetal markets and sells a threat intelligence gateway

system that can be deployed to protect a network and that has various components that can be configured to implement a Network Protect System where those components (e.g., RuleGATE described below) are located at network boundaries and are applying dynamic threat intelligence to network traffic. Ex. 2031.

5. Specifically, Centripetal's threat intelligence gateway system includes three components: RuleGATE, Advanced Cyber Threat, and QuickTHREAT. The RuleGATE product component of the system (which is also offered as a security-as-a-service solution under CleanINTERNET), is a high-performance threat intelligence gateway designed to protect networks from a broad array of threats. RuleGATE instances can be inserted in-line at physical or virtual Internet connections and can be deployed in public or private clouds, on virtual infrastructures, and on a variety of platforms and appliances to enforce intelligence-based security policies, detect possible threats, and stop network attacks. A physical RuleGATE appliance is shown below:



Ex. 2033. In particular, the RuleGATE system can observe in-transit packets to recognize and prevent exfiltrations. The Advanced Cyber Threat ("ACT") system collects and manages millions of unique threat indicators from a combination of Centripetal sources and Centripetal partners. Security expertise is distributed to the gateway system in the form of units of threat intelligence. The QuickTHREAT system is a cyber-threat event analytics system that enables, in part, system administrators to view in real-time the active threat environment in their networks.

One way to summarize Centripetal's product offerings is that CleanINTERNET is a network protection service that Centripetal provides its clients using the RuleGATE platform, the ACT system, and the QuickTHREAT user interface.

6. Centripetal's products prevent a category of cyber-attack known as data exfiltration. Data exfiltrations occur when malware and/or malicious actors carry out an unauthorized data transfer from a computer. For example, a cyber-criminal might steal data such as usernames/passwords, personal information, financial data, or corporate trade secrets, and exfiltrate that data out from a computer or network and into their possession. This problem has been known in the industry since at least 2006, and has been discussed in research papers and trade periodicals, but it was still an ongoing problem. *See Exs. 2007, 2008 (2006 academic paper describing data exfiltrations at length).*

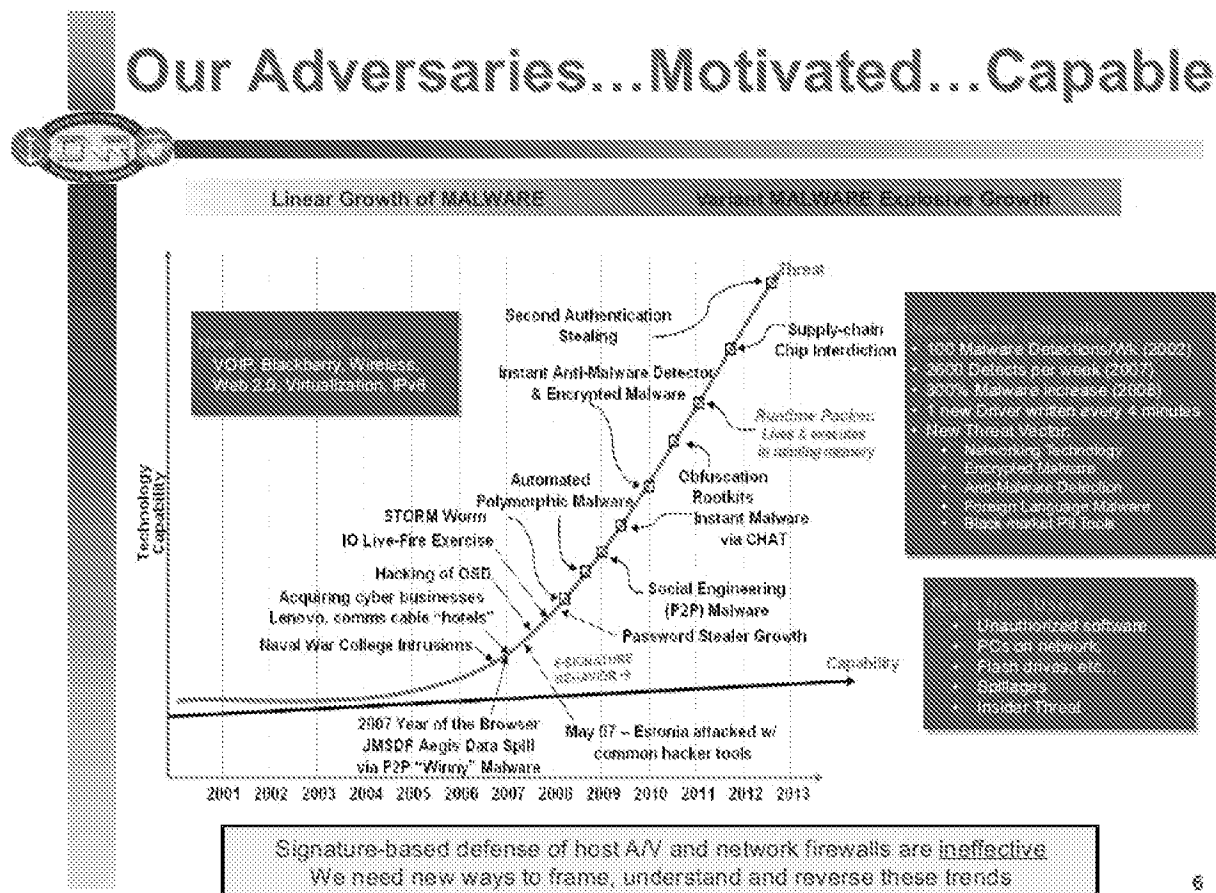
7. We realized that the problem of exfiltrations has been difficult to address because many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the web, that often appear to conventional cyber defense systems as normal network behavior. We also realized that the exfiltration threat was difficult to solve because conventional solutions would block all traffic including legitimate business traffic, which would impede productivity. In addition, conventional cyber defense systems were inadequate and could not scale sufficiently to counter a cyber threat; for example, with respect to traffic volumes, network link speeds, network performance (for example, while still staying within latency and packet loss requirements), network usage policy enforcement, and so forth.

8. With respect to the lack of a sufficiently viable solution, in 2010, the Office of Naval Research announced a program named Proactive Network Defense and Information

Assurance (CND/IA) (Research Opportunity No. 10-004) for funding research into solving the computer network defense program. In connection with this program, the United States Naval Research Laboratory hosted an “Industry Day” event where Stanley Chincheck, the Director for the Navy’s Center for High Assurance Computer Systems, explained in a presentation that previous approaches for protecting computer networks could not keep up with changes in the techniques of malware and malicious actors. Ex. 2013 at 5.

9. In particular, a chart found on page 6 of that presentation is illustrative of the Computer Network Defense program as a whole. The chart’s horizontal axis is time, demarcated in years (from 2000 through 2013) including years 2010-2013 as projected future time, and the chart’s vertical axis represents technological capability. There are two plot graphs in this chart: red and black. The red line represents the technological capability of cyber criminals and the attacks they launch over time. As shown, this graph moves linearly until around the year 2005 or 2006, and then soars, to indicate the explosive (super-linear) growth in the technological capability of cyber criminals. The black line represents the technology capability of computer network defense systems. This graph is nearly horizontal, indicating the flat progress of

conventional network defense systems and their inability to keep up with cyber criminals.



Ex. 2013 at 6. As stated in the yellow box, this chart demonstrated that “[s]ignature-based defense of host A/V and network firewalls are ineffective... we need new ways to frame, understand and reverse these trends.” The failure of signature behavior-based systems, such as the ones disclosed in the Sourcefire reference cited by the Examiner, to keep up with emerging threats demanded new solutions. Accordingly, the need for a scalable solution to the problem of exfiltration attacks was recognized by at least 2010.

10. Conventional network defense systems also failed to provide proactive network protection that could scale to larger networks and meet emerging threats. This was recognized in a white paper entitled “Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-Led Enforcement.” Ex. 2010 at 1. In particular, the

ESG Paper recognized that “[t]he promise of cyber threat intelligence (CTI) for cyber-defense has been talked about for years” and that the manual processes most enterprises have in place for using CTI “don’t scale well and the forensic focus on security emergencies can cause enterprises to miss out on the benefits of proactive, preventive intelligence-based defense.” ESG Paper at 3. The ESG Paper further acknowledged that “[t]he end goal of a threat intelligence program is defense in advance of an event” and identified that “multiple challenges stand in the way of operationalizing threat intelligence in a high performance, and high-fidelity way,” including “[l]ack of automation,” the inability to use feeds “in a meaningful way to live network traffic and even less frequently applied inline for a protective benefit,” and the ability to “turn[] CTI into actionable insight.” Ex. 2010 at 4.

11. Centripetal’s products, including the RuleGATE and CleanINTERNET products, address this problem of exfiltrations because they provide techniques for filtering data between different networks in a manner that greatly curtails the risk of data exfiltration by detecting the threat earlier and acting in response, if desired, while still preserving the flow of normal legitimate network traffic without disruption. It is my understanding that one reason that traditional cybersecurity solutions were ineffective in preventing the exfiltration of data because they required time-expensive inspection of a collection of multiple packets (sometimes referred to as deep packet inspection and/or signature matching) vs. single packets on significant amounts/volumes of high-speed network traffic. Also, prior attempts by others to prevent data exfiltration were often too coarse or overbroad because they would simply block all traffic to/from a given network, regardless of the actual threat, resulting in negative impact to the subject computer network and ultimately to business operations.

12. Centripetal's products allow for deriving network threat intelligence data (from multiple sources) and "operationalizing" cyber threat intelligence (CTI) for protecting networks. RuleGATE leveraged CTI by applying operators only to those packets meeting specific CTI-derived criteria rather than by blocking any and all traffic. This two-stage process succeeds where traditional, overbroad techniques failed because it permits normal business network traffic, like allowing a web browser to download web pages hosted by web servers, but still prevents data exfiltrations. For example, RuleGATE could check outbound traffic for certain types of data transfers that were directed to threat resources (i.e., exfiltrations) and then block those while allowing data transfers to benign/non-threat resources. This is accomplished by applying particular "operators" to different types of traffic based on the criteria of the packets.

13. The ESG Paper discussed above contains industry praise for Centripetal's innovative products. The ESG Paper discussed above praised Centripetal's Threat Intelligence Gateway (TIG) as having "the highest performance network filter that ESG has tested or seen in action to date." Ex. 2010 at 7. The ESG Paper further lauded Centripetal's TIG ability to "deliver[] more than is possible with firewalls and IPS [e.g., Sourcefire] systems", pointing to Centripetal's RuleGATE and CleanINTERNET products:

Centripetal Networks' **CleanINTERNET** intelligence-led managed security service using their **RuleGATE** enforcement point provides customized threat intelligence filtering designed to significantly reduce security event volume and workload in the enterprise. Centripetal shields the network and dynamically monitors for advanced threats using intelligence. **Centripetal's goal is nothing less than the transformation of CTI into protective action at scale. Centripetal does this by converting indicators to rules that drive actions** across a risk spectrum, i.e., logging, content capture, mirroring, redirection, shielding, and advanced threat detection.

Simply put, Centripetal delivers more than is possible with firewalls and IPS systems, which aren't designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds. ESG watched as Centripetal

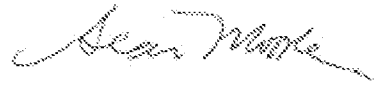
Networks' Threat Intelligence Gateway solution processed over 140 Gbps of network traffic at wire speed; distributing, ingesting, synthesizing into a network policy, and enforcing over five million complex network filtering rules. Each complex filtering rule contained at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state. With intelligence enforcement there can be **no presumption of insider trust** so traditional filters' state assumptions are invalid.

Ex. 2010 at 7 (emphasis added).

14. Centripetal was recognized as an innovator by trade periodicals and analysts. For example, in May 2017, Gartner published its "Cool Vendors in Security for Technology and Service Providers," praising Centripetal as being "unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds." Ex. 2012 at 5. As described in the Cool Vendors article, Centripetal's QuickThreat Gateway "currently has the largest number of third-party threat intelligence service integrations in the network security market. It claims to be able to use up to 5 million indicators simultaneously." *Id.* Centripetal Networks was also named one of American Banker's "Top 10 FinTech Companies to Watch" for 2014 because its Threat Intelligence Gateway, RuleGATE "has the potential to detect and deter rapidly changing cybersecurity threats on the fly." Ex. 2011 at 14.

15. I understand that, in October 2020, Cisco was found to have willfully infringed Centripetal's patents, including U.S. 9,686,193 Patent that is at issue in this reexamination proceeding. Ex. 2032. I testified as a fact witness at this trial. I understand that the judge determined that Cisco deliberately copied Centripetal's technology. Specifically, the judge found that Cisco met with Centripetal to express interest in Centripetal's proprietary technology, then appropriated the information it learned at those meetings and embedded the technology into its own products. Ex. 2032.

16. I have I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on January 25, 2020 in Portsmouth, NH.

A handwritten signature in cursive script, appearing to read "Sean Moore".

Sean Moore