CYBERCRIME REPORT
Q2 - JULY 2021

Arete

Crime and No Punishment

Impunity Breeds Innovation and Aggression

If you can’t do the time, don’t do the crime.

If only this idiom held true in the cyber realm. Left unchecked, state-sponsored actors and cybercrime groups have had no reason to pull back and instead, have become more aggressive, marking a paradigm shift across the cyber landscape in Q2 2021. The most flagrant examples are recent supply chain and managed service provider (MSP) compromises, a longstanding nation state stratagem now co-opted by organized cybercriminal elements operating freely within regimes that turn a blind eye to cybercrimes launched from within their own borders.

Naturally, Western democratic leaders are racing to define boundaries on the ever-blurring line between organized crime and national security threats. The rule book is now being written — only, it’s always far more difficult to define and enforce a boundary after the fact. Thus, the strategies and actions of government leaders and the cybersecurity community will be vigorously tested in the coming months as many of these threat actors have operated with relative impunity over the last decade, using this time and freedom to innovate, continually refine their techniques, and become even more efficient in their malicious endeavors.

Q2 2021 highlights from Arete’s incident response cases[1]

- Cybercriminals exploiting vulnerabilities first observed in cyber-espionage campaigns.
- Ransomware operators primarily targeting the professional services, public services, and healthcare industries.
- Ryuk ransomware operators collected the highest average ransomware payment (US$915,000) over Q2.

Other key cybersecurity events in Q2 2021

- U.S. President Joe Biden signed an executive order directed at improving cybersecurity posture across the public and private sectors.[2]
- North Atlantic Treaty Organization (NATO) members discussed applying Article 5 Collective Defence[3] to cyberattacks.
- Law enforcement action extended beyond takedowns of malware botnets and underground shops.

What to expect

- Expect to face the challenges of unforeseen cascading effects from recent devastating compromises involving Microsoft Exchange, SolarWinds, Codecov, and PulseVPN.
- Expect to see attacks increase in intensity in the near-term, bearing similar consequences to those of the FireEye, Microsoft, Colonial Pipeline, JBS, and Kaseya compromises.
- Expect to see more erratic upheaval and “unexplained” disruption to cyber threat actor operations as world leaders take more furtive, albeit clandestine, measures to combat recent cyberspace transgressions. There are many lines to draw — each will be dependent on context and with varying degrees of retribution.

[1] Disclaimer: Unless otherwise noted, all data within this report is based on Arete incident response cases.

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[3] https://www.nato.int/cps/en/natohq/topics_110496.htm

Threat actors innovating to accelerate ransomware gains

Like legitimate businesspeople, threat actors are always looking for ways to optimize operations and boost profits. With time and impunity on their side, some creatively approached things in Q2 2021.

DATA AS HOSTAGE

In April 2021, Arete provided a forecast on the future of cybercrime, coining the term Data as Hostage (DasH).[4]

Evidence shows that threat actors are shifting tactics, spending less time and resources encrypting victim data and instead, simply exfiltrating and holding valuable information for ransom.

DasH requires less overhead for threat actors as they don't need to produce or procure ransomware. At the same time, it increases risk for victims as the mean time to detect (MTTD) data breaches is 197 days.[5]

In May 2021, Babuk ransomware operators put this strategy into action, publicly announcing a cessation of ransomware and expressing their intent to focus on raiding victim environments and exfiltrating data.

DUAL ENCRYPTION

The gig economy has a doppelganger in the cybercrime marketplace. Just as an Uber driver can also be a Lyft driver, a ransomware operator can optimize the return on their intrusion labor by driving operations for multiple Ransomware-as-a-Service (RaaS) platforms.

During Q2 2021, Arete aided several organizations in their recovery of dual-encryption instances involving multiple ransomware variants. Given our unique visibility, Arete observed this behavior most pronounced with HelloKitty ransomware affiliates.

- Dharma (Dharma + Waiting)
- Arcane (Arcane + Crylock)

April 2021 - HelloKitty ransomware operators:

- HelloKitty + Conti
- HelloKitty + Babuk
- HelloKitty + SunCrypt

In addition to this primary assertion, several other factors may be relevant to understanding why dual-encryption scenarios occur, including:

- Multiple threat actors compromising victims through a common initial access vector — for example, a ProxyLogon vulnerability — within a short timeframe.
- Threat actors actively cooperating with one another to consolidate resources and time investment.
- Threat actors operating different ransomware and targeting victims with the same profile — for example, the same sector or business type.

[4] https://www.areteir.com/dash-into-the-future-of-cybercrime/

[5] https://www.csoonline.com/article/3544911/real-time-matters-in-endpoint-protection.html

Threat actors innovating to accelerate ransomware gains

LEVERAGING ZERO DAYS

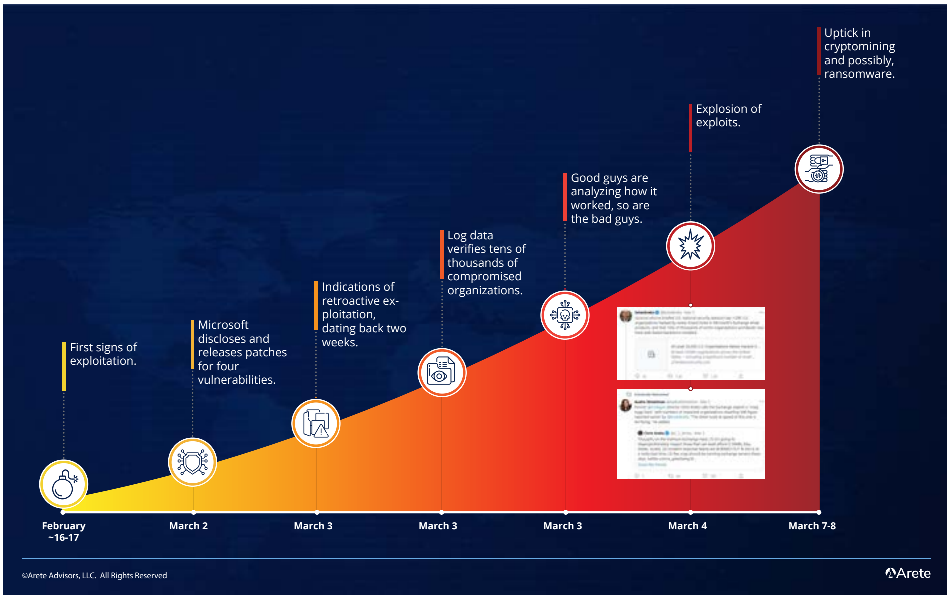
In Q2 2021, Arete observed cybercrime actors quickly adopting the use of exploits targeting zero-day vulnerabilities — for example, ProxyLogon and Pulse VPN. This exploitation followed initial use by suspected state-sponsored actors conducting likely cyber-espionage campaigns.

ProxyLogon

On March 23, 2021, Microsoft released a report detailing the intrusion tactics, techniques, and procedures (TTPs) of HAFNIUM, a suspected Chinese state-sponsored cyber threat group. In tandem with the report, the company released patches for the ProxyLogon vulnerability disclosures CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065.

HAFNIUM leveraged these vulnerabilities to execute remote code that broadly impacted privately operated on-premises Microsoft Exchange servers.

MICROSOFT EXCHANGE ZERO-DAY SERVER HACK


First signs of exploitation.
Microsoft discloses and releases patches for four vulnerabilities.
Indications of retroactive exploitation, dating back two weeks.
Log data verifies tens of thousands of compromised organizations.
Good guys are analyzing how it worked, so are the bad guys.
Explosion of exploits.
Uptick in cryptomining and possibly, ransomware.
February ~16-17
March 2
March 3
March 3
March 3
March 4
March 7-8
©Arete Advisors, LLC. All Rights Reserved
Arete

Arete responded to 100+ incidents involving the use of the ProxyLogon vulnerabilities. Multiple researchers and cybercrime threat actors, including ransomware operators like Black Kingdom, DearCry, and REvil, leveraged ProxyLogon exploits to gain access to victim networks shortly after the HAFNIUM disclosure.

Pulse Secure VPN

During Q2 2021, Microsoft Threat Intelligence also disclosed critical vulnerabilities in Pulse Secure VPN that cybercriminals used to facilitate intrusions.

Specifically, Arete observed HelloKitty and Black Kingdom[6] ransomware operators exploiting unpatched instances of Pulse VPN to establish initial access to victim networks.

Once they had initial access, they likely continued the intrusion cycle by escalating privileges and moving laterally to gain control of the domain controller and deploy their ransomware across the enterprise network for maximum impact.

[6] https://www.areteir.com/black-kingdom-returns-to-exploit-zero-day-vulnerabilities-in-unpatched-microsoft-exchange-servers/

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Arete

Cyber Emergency Helpline 866 210 0955
Phone 646 907 9767

New Engagements
Arete911@AreteIR.com

www.areteir.com

Arete Advisors, LLC makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the contents of this report and expressly disclaims liability for errors and omissions in the content. Neither Arete Advisors, LLC, nor its employees and contractors make any warranty, express or implied or statutory, including but not limited to the warranties of noninfringement of third-party rights, title, and the warranties of merchantability and fitness for a particular purpose, with respect to content available from this report. Arete Advisors, LLC assumes no liability for any direct, indirect, or any other loss or damage of any kind for the accuracy, completely, or usefulness of any information, product, or process disclosed herein, and does not represent that the use of such information, product, or process would not infringe on privately owned rights.