

**CYBERCRIME
REPORT**
Q2 - JULY 2021



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 cases¹

- 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 Defence³ 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



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 Kingdom⁶ 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/>

THE HISTORY OF THE UNITED STATES

THE AMERICAN REVOLUTION

The American Revolution was a period of political and social change in the United States. It began in 1775 and ended in 1783. The revolution was fought between the thirteen original colonies and Great Britain. The colonies won independence and became a new nation.

The revolution was a result of the colonies' desire for self-government. They were tired of being ruled by Great Britain. They wanted to make their own laws and elect their own leaders. The revolution was a success because the colonies won their independence.



THE AMERICAN CIVIL WAR

THE CAUSES OF THE CIVIL WAR

The American Civil War was fought between the Union and the Confederacy from 1861 to 1865. The war was caused by the issue of slavery. The Union wanted to abolish slavery, while the Confederacy wanted to keep it.

The war was a result of the growing divide between the North and the South. The North was becoming more industrial and more concerned with the rights of all people. The South was becoming more agricultural and more concerned with the rights of white people.



Environment: air, water, pollution, conservation

The environment is a complex system of interacting elements. It includes the air, water, land, and living organisms. The environment is constantly changing, and human activities have a significant impact on it. We need to understand the environment and how it works in order to protect it and ensure a sustainable future for ourselves and future generations.

Air Quality and Pollution

Air quality is a measure of the cleanliness of the air. It is affected by a variety of factors, including natural sources like wind and weather, and human activities like burning fossil fuels and industrial processes. Air pollution can have serious health effects, including respiratory problems and heart disease. It can also damage the environment and contribute to climate change.

There are several ways to improve air quality. One way is to reduce the amount of pollution that is released into the air. This can be done by using cleaner technologies and processes, and by encouraging people to use public transportation or carpooling. Another way is to plant more trees, which can help to absorb pollutants from the air.

Water is a vital resource for all life. It is essential for drinking, growing food, and many other activities. However, water is becoming increasingly scarce in many parts of the world. This is due to a variety of factors, including population growth, climate change, and pollution. We need to take steps to protect our water resources and ensure that we have enough clean water for the future. One way to do this is to conserve water by using it more efficiently. This can be done by taking shorter showers, turning off the tap when brushing teeth, and using water-saving devices. Another way is to protect watersheds, which are the areas of land that drain into a body of water. By protecting watersheds, we can help to ensure that the water that flows into them is clean and healthy.

Land is another important resource. It is the source of food, shelter, and many other things that we need to survive. However, land is being lost at an alarming rate due to deforestation, urbanization, and other human activities. We need to take steps to protect our land resources and ensure that we have enough land for the future. One way to do this is to plant more trees, which can help to prevent soil erosion and improve the quality of the land. Another way is to use land more efficiently by building more compact communities and reducing the amount of land that is used for agriculture and other purposes.

Conservation is the practice of protecting and managing natural resources. It is essential for ensuring that we have enough resources for the future. There are many ways to conserve resources, including recycling, using energy efficiently, and protecting natural areas. By conserving resources, we can help to ensure a sustainable future for ourselves and future generations.

Pollution is the introduction of harmful substances into the environment. It can have serious health effects, including respiratory problems and heart disease. It can also damage the environment and contribute to climate change. There are many ways to reduce pollution, including using cleaner technologies and processes, and encouraging people to use public transportation or carpooling. By reducing pollution, we can help to protect our health and the environment.

Conservation and pollution are two sides of the same coin. We need to take steps to protect our resources and reduce pollution in order to ensure a sustainable future for ourselves and future generations. By working together, we can make a difference and create a better world for everyone.

THE AMERICAN WEST

The American West was a region of the United States that was characterized by its vast, open spaces and its rich natural resources. It was a region that was often the site of conflict between different groups of people, including Native Americans, settlers, and the military. The West was also a region that was often the site of exploration and discovery, and it played a key role in the development of the United States.

THE AMERICAN WEST: A REGION OF CONFLICT AND DISCOVERY

The American West was a region of the United States that was characterized by its vast, open spaces and its rich natural resources. It was a region that was often the site of conflict between different groups of people, including Native Americans, settlers, and the military. The West was also a region that was often the site of exploration and discovery, and it played a key role in the development of the United States.

The American West was a region of the United States that was characterized by its vast, open spaces and its rich natural resources. It was a region that was often the site of conflict between different groups of people, including Native Americans, settlers, and the military. The West was also a region that was often the site of exploration and discovery, and it played a key role in the development of the United States.

THE AMERICAN WEST: A REGION OF CONFLICT AND DISCOVERY

The American West was a region of the United States that was characterized by its vast, open spaces and its rich natural resources. It was a region that was often the site of conflict between different groups of people, including Native Americans, settlers, and the military. The West was also a region that was often the site of exploration and discovery, and it played a key role in the development of the United States.

THE AMERICAN WEST: A REGION OF CONFLICT AND DISCOVERY

The American West was a region of the United States that was characterized by its vast, open spaces and its rich natural resources. It was a region that was often the site of conflict between different groups of people, including Native Americans, settlers, and the military. The West was also a region that was often the site of exploration and discovery, and it played a key role in the development of the United States.

Page 1 of 1



Page 1 of 1

Page 1 of 1

Page 1 of 1

Page 1 of 1

1. 2019年1-12月中国主要城市空气质量



2019年1-12月中国主要城市空气质量分布图



2019年第一季度、第二季度、第三季度中国主要城市空气质量分布图



2019年第四季度及全年中国主要城市空气质量分布图



How to Use the Security Guard's Log

The Security Guard's Log is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift.

The Security Guard's Log is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift.

The Security Guard's Log is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift.

The Security Guard's Log is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift.

The Security Guard's Log is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift. It is a document that is used to record the activities of the security guard during their shift.



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.