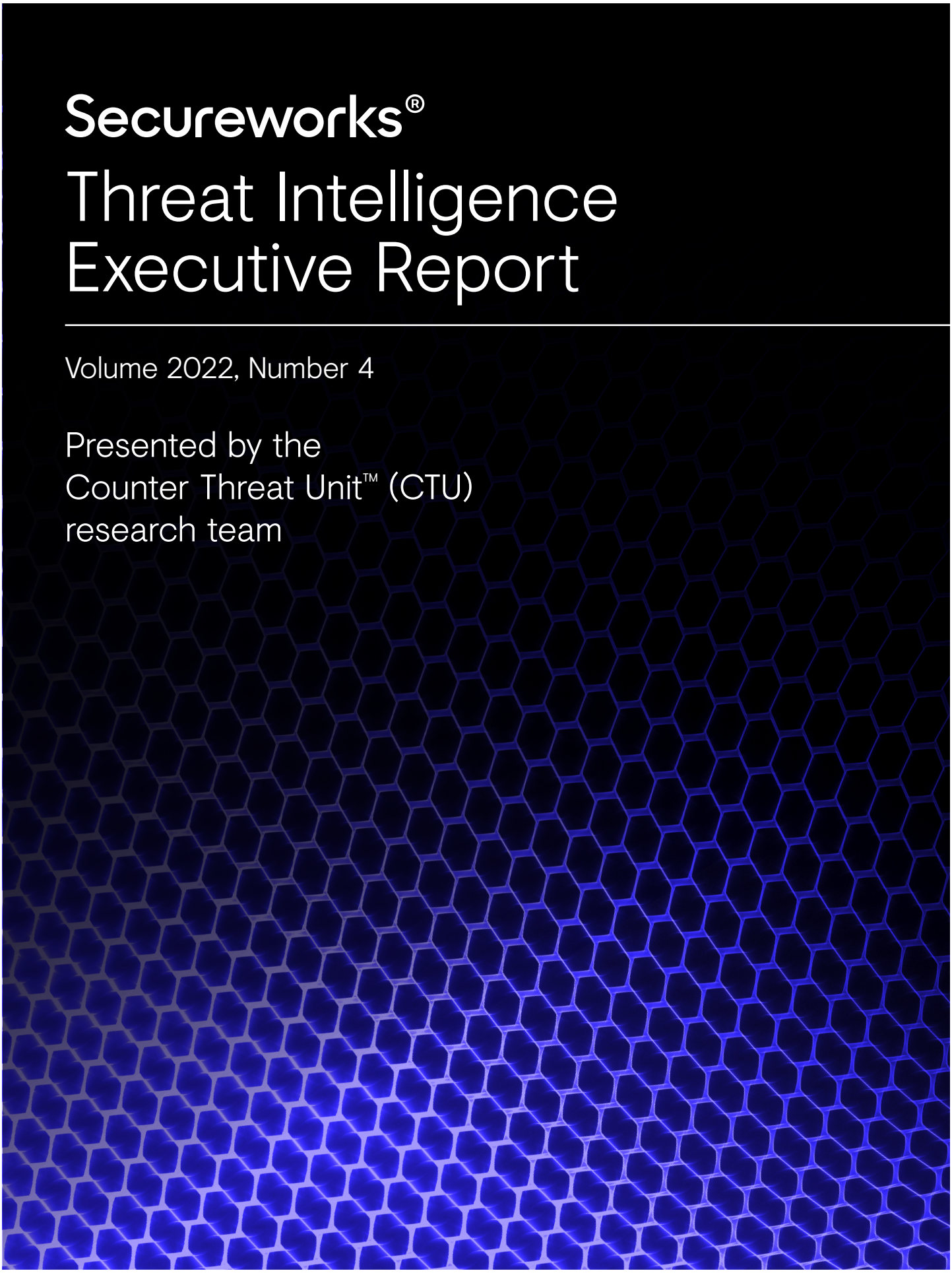
Secureworks®

Threat Intelligence Executive Report

Volume 2022, Number 4

Presented by the
Counter Threat Unit™ (CTU)
research team



Executive Summary

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats to help organizations protect their systems. During May and June, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Government-sponsored threat groups use ransomware too
- Don't leave the door to your data unlocked
- Business email compromise (BEC) is as big a problem as ransomware

Government-sponsored threat groups use ransomware too

Not all ransomware is financially motivated. Sometimes other motivations are at play.

The ransomware ecosystem is highly changeable. Ransomware variants come and go, in some cases accumulating only a handful of victims before disappearing. While most ransomware activity is opportunistic and focused on making money, some patterns suggest other motivations. Keeping track of the evolving landscape is an important part of what the CTU research team does.

CTU researchers identified a cluster of five ransomware families and attributed them to the Chinese BRONZE STARLIGHT threat group. All the families were short lived, did not operate an affiliate model, and were linked through code overlap and common use of the HUI Loader malware.

HUI Loader is also associated with intellectual property (IP) attacks carried out by the Chinese government-sponsored BRONZE RIVERSIDE threat group. Shared use of this tool indicates a relationship between BRONZE STARLIGHT and BRONZE RIVERSIDE, suggesting that BRONZE STARLIGHT might be a government-sponsored threat group that could be motivated by IP theft and cyberespionage rather than financial gain.

Government-sponsored threat groups from countries such as Iran and North Korea have also used ransomware. However, motivations vary. North Korean attacks are likely financially motivated to raise sanction-bypassing funds for the economy, while Iranian threat groups often conduct destructive and irreversible encryption activity under the pretext of ransomware.

These revelations underline the importance of understanding intent when responding to an incident, so that the potential impact can be fully quantified.

What you should do next:
Make sure that you know what data you have, and understand who might be interested in it. For context, ensure that your incident response team or provider has access to the latest threat intelligence.

Don't leave the door to your data unlocked

All too often, corporate data is left unsecured and open to external access. Widely available internet tools make it trivial for threat actors to discover and compromise this data.

In June 2022, CTU researchers reported that over 1,200 Elasticsearch databases had been replaced by a ransom note demanding a Bitcoin payment in exchange for the data. In every case, the databases were public and required no authentication to access. While the scale of this attack might initially appear staggering, it is unsurprising given the existence of freely available and simple-to-use internet search tools like Shodan that can quickly identify this type of unsecured data.

This tactic of exploiting unsecured databases for data theft and extortion is widespread. It is relatively trivial for opportunistic threat actors to build searches to identify internet-exposed data that they can steal.

Too often, organizations fail to secure important corporate assets because of the mistaken assumption that the assets are hard to find or access by anyone other than a small number of legitimate users. The other common mistake organizations make is leaving API authentication keys exposed in publicly accessible code repositories such as GitHub. Threat actors are well aware of this and are familiar with the freely available tools for finding and stealing these keys, which should always be kept secret.

What you should do next:
Check whether internet-facing databases need to be internet-facing. If so, implement multi-factor authentication. Ensure that API keys that provide programmatic access to these data assets are not inadvertently exposed.

Business email compromise (BEC) is as big a problem as ransomware

Ransomware gets the headlines, but the reality is that BEC attacks account for higher monetary losses because there are so many of them. BEC attacks keep growing in number and believability, and they are not going away any time soon.

In May, as part of Interpol's Operation Delilah, Nigerian police arrested an individual believed to be the leader of the SilverTerrier/TMT BEC syndicate. SilverTerrier is associated with BEC activity dating back to 2015. Its attacks have impacted thousands of businesses and individuals across four continents.

CTU researchers observe BEC threat actors in 2022 using the same tactics and techniques they have used for a decade, because they work. The most common BEC techniques involve the compromise of user email accounts. These techniques are quick and easy if organizations aren't protecting themselves, and they don't require the threat actors to build or deploy malware. And the cost for the victim can easily exceed a million U.S. dollars.

BEC attacks target business processes as much as technology. Financial controls are imperative to ensure that organizations carefully validate payment details before making a financial transaction. Technical controls can also play a part. Implementing multi-factor authentication can mitigate attacks, and reviewing logs can detect unauthorized account logons or the creation of unusual mail-forwarding rules.

A successful BEC attack can cost a victim a considerable amount of money. Secureworks incident responders consistently advise organizations to secure email and to monitor for spoofed domains, which are often leveraged in these attacks.

What you should do next:
Implement multi-factor authentication for remote access to platforms such as Microsoft 365. Check that your monitoring tools cover telemetry from your cloud infrastructure. Test your business processes for verifying and approving large-value corporate payments.

Conclusion

Not all cyberattacks are difficult to conduct, and easily available tools help threat actors detect potential victims. Successful defense depends on keeping security front of mind in both business process design and technology implementation. It also requires an expert and current understanding of the threat landscape.

A glance at the CTU research team

CTU researchers frequently serve as expert resources for the media, publish technical analyses for the security community, and speak about emerging threats at security conferences. Leveraging Secureworks' advanced security technologies and a network of industry contacts, the CTU research team tracks threat actors and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables CTU researchers to identify threats as they emerge and develop countermeasures that protect customers before damage can occur.

Research

Understanding the nature of threats customers face, and creating countermeasures to address and protect.

Intelligence

Providing information that extends the visibility of threats beyond the edges of a network.

Integration

Infusing CTU research and intelligence into Secureworks managed security services and security consulting practices.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086

Japan
Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

If you need immediate assistance, call our 24x7 **Global Incident Response Hotline:**

+1-770-870-6343

