Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2023, Number 1

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 November and December, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Adapt for impact – what 2022 tells us about ransomware in 2023
- Ukraine isn't the only target for cyberespionage groups
- Cyberattacks against NGOs threaten life and liberty

ADAPT FOR IMPACT – WHAT 2022 TELLS US ABOUT RANSOMWARE IN 2023

Ransomware activity slowed during 2022 in some respects, but threat actor adaptability did not. Continuing and evolving attacks are likely in 2023.

For the first time in several years, there was no significant year-on-year increase of name-and-shame ransomware attacks in 2022. The number of victims listed on leak sites remained roughly static. There were fewer extremely high-profile attacks like Colonial Pipeline. Incidents that made headlines, such as the Conti attack on Costa Rica, appeared to draw less law enforcement attention. Secureworks incident responders also observed fewer attacks that encrypted entire networks. Some of the reasons fueling these trends will affect attack numbers for 2023 too.

The war in Ukraine seems to be the most obvious factor, as it has disrupted lives in Russia and especially Ukraine. Although cybercrime has historically been linked to Russia, many cybercriminals were based in Ukraine where nearly all men under the age of 60 have become eligible for mobilization. As the conflict continues into 2023, it may continue to somewhat depress ransomware attack numbers.

Organizations may also be getting better at detecting ransomware precursor activity and stopping attacks before they take hold. Perhaps in response, threat actors updated their arsenals and diversified their tooling. In 2021, Cobalt Strike was ubiquitous as an offensive security framework, whereas in 2022 CTU researchers increasingly observed the use of alternatives like Brute Ratel. Additional tooling adjustments are likely in 2023. These changes could include increased use of other offensive security tools and more efforts to design ransomware that is faster, cross-platform, and difficult to detect. As organizations improve their detection capabilities, threat actors must shorten the time between initial access and ransomware deployment to hours rather than days.

Improved detections likely also led threat groups to diversify their tactics, particularly regarding extortion that relies on data theft without encryption. It originally seemed unlikely that data theft alone would compel victims to pay ransoms, but these attacks increased. In particular, the GOLD RAINFOREST threat group (also known as Lapsus$) carried out high-profile heists on tech companies such as Microsoft.

Threat actor benefits from this pared-down approach include a lower development and maintenance burden, faster attacks with fewer opportunities for detection, and less negative publicity, especially when attacking sensitive targets like hospitals. This trend will likely continue through 2023 if threat actors consider the lower effort and risk worth the potentially smaller ransom payments. These data theft-only attacks were by no means the norm but provide another sign that ransomware attackers adapt and diversify to stay effective.

What you should do next:
Subscribe to well-respected threat intelligence feeds to stay up to date and protected against the latest ransomware tactics, techniques, and procedures.

UKRAINE ISN'T THE ONLY TARGET FOR CYBERESPIONAGE GROUPS

Russian state-sponsored threat actors conduct broad cyberespionage campaigns for political and economic gain.

For most of 2022, Russia and the rest of the world focused on Ukraine. Much of the Russian IRON FRONTIER cyberespionage group's activity was driven at least in part by the conflict. The group conducted espionage campaigns against non-governmental organizations (NGOs), weapons suppliers, and logistics providers that directly support Ukraine.

However, IRON FRONTIER doesn't focus exclusively on Ukraine. For example, the threat actors reportedly targeted high-profile pro-Brexit supporters in the UK, including the former head of MI6, to reinforce division in the country.

In addition, CTU researchers uncovered infrastructure exposing a long-running IRON FRONTIER spearphishing campaign targeting staff at three U.S. national laboratories: Argonne National Laboratory, Brookhaven National Laboratory, and Lawrence Livermore National Laboratory. These laboratories are linked to the U.S. Department of Energy and conduct advanced scientific research on many topics of considerable strategic and economic importance to the U.S., including nuclear energy and quantum information science research. Nuclear research could be of interest to Russia as Russian President Vladimir Putin is threatening nuclear strikes in Ukraine, but these laboratories also conduct other energy-related research that would be broadly useful to Russia.

Russia is not the only country conducting cyberespionage operations. China has been the subject of coordinated warnings from the UK, the U.S., and other Five Eyes nations due to its regular economic cyberespionage activities. These attacks included intellectual property theft under the guise of ransomware attacks. In 2020, the U.S. Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) warned about the danger that Chinese threat actors posed to COVID-19 research in the U.S. In addition, specific Chinese threat groups steal intellectual property from Japanese organizations.

The threat of espionage is not limited to research labs. All organizations should periodically evaluate whether their activities, their stored data, and their business partners could make them a target for espionage. They should then factor these risks into their threat model and security control framework.

What you should do next:
Review your operational risk calculations, factoring in the latest geopolitical situations without making them the only consideration. Crises may drive some state-sponsored threat group activity but do not solely determine tasking.

CYBERATTACKS AGAINST NGOS THREATEN LIFE AND LIBERTY

State-sponsored threat groups maintain a keen interest in the activities of dissidents and those who support them.

In December 2022, Amnesty International Canada and Human Rights Watch (HRW) became the latest in a long line of NGOs to publicly acknowledge state-sponsored attacks against their IT networks. Amnesty's statement, which was based on a forensic investigation conducted by Secureworks, revealed that a Chinese threat actor compromised Amnesty's networks to search for specific information relating to Chinese individuals of interest. The attacker gathered information about Amnesty's previous interactions with those individuals and then monitored plans for further engagement.

Iranian threat groups also often attempt to gain intelligence about individuals of interest to their regime, including those involved with NGOs. HRW described how threat actors backed by the Iranian government targeted two HRW staff members and at least 18 other high-profile individuals in a social engineering and credential phishing campaign during October and November 2022. These targets included activists, journalists, researchers, academics, diplomats, and politicians working on Middle East issues.

Repressive regimes regularly conduct surveillance against individuals and organizations whose actions are viewed as contrary to the regime's strategic ambitions. At risk are NGOs, journalists, academics, and other organizations and individuals involved in or reporting on dissent against these regimes. The threat actors often conduct a phishing attack or use another form of social engineering to obtain an individual's credentials that provide system access. The organizations and individuals at highest risk regularly field unsolicited communications as part of their job, so restricting interactions is not feasible. However, organizations should educate users about common phishing tactics to reduce risk.

What you should do next:
Train users to recognize phishing attempts, and implement technological controls such as restricting access to unauthorized websites and enabling multi-factor authentication. Comprehensive monitoring can provide early detection of successful attacks.

CONCLUSION

The threat landscape is ever evolving, driven by multiple factors. Staying alert to changes in geopolitical pressures and threat actor behaviors is an essential part of cyber defense.

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 global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

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

