Secureworks®

THREAT INTELLIGENCE EXECUTIVE REPORT

Volume 2023, Number 6

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. Based on observations in September and October, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Israel-Hamas war presents specific cyber risks
- Preparation is the best defense against distributed denial of service (DDoS) attacks
- Underground forums posts reveal threat actor intent

ISRAEL-HAMAS WAR PRESENTS SPECIFIC CYBER RISKS

The current risk to most organizations is low, but preparation and good cyber hygiene are always worthwhile choices.

The ongoing war between Ukraine and Russia demonstrates that modern kinetic warfare is increasingly accompanied by hostile cyber activity. However, so far, the cyber element of the Israel-Hamas war that started on October 7 has been limited, consisting primarily of hacktivist activity on both sides. At least 100 hacktivist groups were identified by late October, and the majority were pro-Palestinian. Most hacktivist efforts have focused on distributed denial of service (DDoS) attacks and website defacements.

There is limited evidence to support claims of more sophisticated attacks against critical national infrastructure and military targets, but that could change. Both Israel and Hamas have longstanding cyber capabilities, and groups linked to countries such as Russia and Iran are getting involved in the conflict. Iran in particular has a long history of state-sponsored threat groups attacking Israeli interests via hack-and-leak, wiper, and ransomware tactics, as well as employing fake cybercrime and hacktivist personas. Iranian attacks and support of proxy interests throughout the Middle East will continue regardless of the war. There are also indications that Iran is striving to provoke radical anti-Israeli activity in other countries and online, which could further increase hacktivism.

Organizations that have high-profile links to either side of the conflict or that engage in humanitarian efforts in the region are most at risk from hacktivist activity. However, most hacktivist attacks are short-lived and easily defended against. Implementing good cyber hygiene and engaging a DDoS mitigation service are essential preparations for organizations that may be at risk.

✓ **What you should do next:**
Ensure that your incident response plan is up to date and relevant to current threats.

PREPARATION IS THE BEST DEFENSE AGAINST DDOS ATTACKS

DDoS attacks are usually a nuisance rather than an existential threat, but they are surging in prevalence and power. Being prepared is key.

DDoS attacks are favored by hacktivist groups and have been widely used in the Russia-Ukraine and Israel-Hamas wars. Hacktivists often target entities that have opposing ideologies, organizations that support those entities, or even other threat actors. Additionally, ransomware groups sometimes pressure victims to pay by threatening DDoS attacks.

According to a September Europol report, the pro-Russia hacktivist group KillNet claimed responsibility for the "most outstanding" DDoS attacks against European Union targets during 2022. The report reveals that another pro-Russia group called NoName057 operates a crowdsourced botnet project named DDOSIA, which pays participants to install a DDoS bot on their own systems. NoName057 conducted DDoS attacks against French legislative bodies earlier in 2023.

DDoS attacks are intended to overwhelm websites and other internet properties such as API gateways with more traffic than they can handle at once. In the third quarter of 2023, the largest attack ever recorded peaked at 201 million requests per second. That record will likely be broken, as traffic volumes continue to climb. In the past, DDoS botnets were largely composed of infected internet of things (IoT) devices. Now, they may include virtual machines on cloud computing platforms. DDoS-for-hire platforms are widely advertised on underground forums. At the beginning of September, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released guidance to help Federal Civilian Executive Branch (FCEB) agencies evaluate and mitigate the risk of DDoS attacks against their websites and related web services.

DDoS attacks generally cause more inconvenience than permanent damage. Organizations concerned about system downtime resulting from these attacks should engage DDoS mitigation services in advance because attacks that are already underway are difficult to counter.

✓ **What you should do next:**
Read the CISA guidance for information about available mitigation services

UNDERGROUND FORUMS POSTS REVEAL THREAT ACTOR INTENT

Monitoring platforms where threat actors interact and do business provides intelligence that protects customers.

CTU researchers monitor underground marketplaces and forums to obtain intelligence on active threat actor operations around the world. Monitoring these forums, along with messaging channels such as Telegram, reveals a wide range of insights about threat actors' activities. The insights produce a rich, rounded view of the threat landscape.

Threat actors' posts can reveal information such as targets of interest and overlaps between hacktivist and cybercriminal activity. For example, posts during the reporting period demonstrated how making assumptions about threat actors' areas of focus can lead to overlooking potential threats. Hacktivists from both sides of the Russian-Ukraine war discussed working together to conduct ransomware and data extortion attacks. Two days after the October 7 Hamas attack on Israel, ransomware actors requested access to systems in Iran, Palestine, or Gaza-affiliated countries and then later advertised a data dump of purported Palestinian health records they had obtained.

CTU researchers additionally observed numerous threat actors seeking stolen credentials for a hotel booking service's property management portal. These observations provided a deeper understanding of an ongoing campaign that targets hotel guests' payment information.

Forum posts regularly advertise access to compromised organizations, which can warn potential victims about ransomware attacks before they occur. Threat actors also offer exploits for sale, identifying which vulnerabilities organizations should prioritize patching. The monitoring can also reveal types of systems that are typically used for illicit access, as well as details about threat actors' tactics, techniques, and procedures. Many posts advertise stolen databases and new malware and can assist with attribution of threat actor activity.

CTU researchers immediately notify Secureworks customers of identified references to their organizations. The CTU research team channel observations and insights into Secureworks Taegis™ detections and threat intelligence publications.

✓ **What you should do next:**
Study CTU threat intelligence publications for context when making risk assessment and resource allocation decisions.

CONCLUSION

Defending against cyberattacks is all about preparation. Proper preparation can limit the impact of some attacks, including DDoS activity. Proactively sealing initial access vectors that result from unpatched systems or unsecured remote services can stop other attacks in their early stages. Preparation may seem expensive or onerous, and tolerating DDoS attacks is the right choice for some organizations. For ransomware, wiper, or cyberespionage attacks, informed preparation is essential and is often less expensive and lower impact than dealing with the aftermath of an attack.

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 intelligence into the Secureworks Taegis XDR platform, managed solutions, and security consulting practices.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of over 4,000 organizations around the world who use its advanced, AI-driven capabilities 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