Threat Intel Report

Prepared by:

CBI Threat Intel Group

March 8, 2022

securityalert@cbisecure.com | 800.747.8585

Modern warfare is waged on more than one front: There's physical warfare, there's the economic front, and there's the cyber dimension. As recent geopolitical events underscore, these spheres are intertwined. Activity in one area impacts the others, and conflicts between nations can directly or indirectly affect an organization's operations as well as its reputation in the eyes of customers and partners.

The war in Ukraine has generated heightened interest in the topic of cyber security. While we should have paid attention to cyber hygiene all along, it's not surprising that it takes outright conflict in the physical world to make potential cyber impacts more real in our minds.

As organizations, we must fortify our security posture to be able to identify, detect, mitigate, and protect from attacks on all fronts. Recent events underscore the importance of creating a crisis management plan. The more prepared an organization is for an unforeseen event, whether physical or in the cyber realm, the more manageable any crisis will be.

Emerging Trends

War in Ukraine

As mentioned in last month's report, the geopolitical tensions between Russia and Ukraine have already spilled into the cyber realm, and now with the two countries at war, cyber activity has only escalated. Because the effects of the conflict could potentially spread to companies without a tie to Ukraine, companies should heed a recent CompTIA warning to prepare for disruptive attacks on their networks as well as those of customers, suppliers and partners.

Strains of malware currently tied to the Ukraine conflict:

- IsaacWiper and HermeticWizard, disclosed on March 1
- HermeticWiper, a data wiper disclosed on February 23
- WhisperGate, a destructive MBR-locking malware disclosed on January 15

Although these specifically target Ukrainian firms, any organization that partners or associates with an affected Ukrainian business is at risk.

The conflict has created obvious challenges for companies with offices, employees or contractors in Ukraine. The country is one of the top IT outsourcing destinations globally, with numerous Fortune 500 companies among clients served, and is home to a number of tech startups. Protecting employees, contractors and assets must be the top priority for companies that rely on Ukrainian talent.

While many have speculated as to why Russia hasn't yet launched a full scale cyber attack on Ukraine, the chairman of Ukraine's cyber security ministry said attacks are happening but Ukraine is defending against them. The Ukrainian government has also called for volunteer hackers to protect from cyber attacks and to conduct digital espionage.

The hacktivist group Anonymous has summoned its members to attack Russian government targets, while certain ransomware groups have made their loyalty to Russia clear. It's anyone's guess which direction the conflict will take from here, but we can certainly expect cyber ramifications and should remain ever watchful of the threat to critical infrastructure.

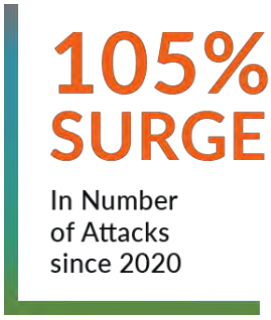
Threats & Attacks

Malware and Malvertisement

While 2021 saw some malware families retire, it also saw the return of a few devastating strains. One of those is Emotet, which topped Check Point's list of the most prevalent malware so far this year and is often used as a distributor for other malware. Emotet, seen impacting 6% of organizations, was followed by the Trickbot banking Trojan (which has since shut down); the Formbook infostealer; and Agent Tesla, an advanced RAT.

On the Mac OS side, the Center for Internet Security has consistently observed that infection via malvertisement has been a prominent attack vector. Malvertisements, or advertisements into which attackers have injected malicious code, may be found on malicious sites, as well as legitimate sites, including social media, entertainment, news and various other media platforms. To combat malvertising, organizations should have policies for approved software.

Ransomware Groups Shift Focus, Expand Partnerships



Since the Biden administration's 2021 decision to aggressively crack down on ransomware threat actors, these malicious groups have scaled back some of their activity, but even still, according to a February SonicWall report, ransomware attacks in 2021 outpaced previous years. The number of attacks in 2021 surged by 105% since 2020 and by 232% since 2019.

A recent CISA alert highlighted an increase in ransomware incidents against critical infrastructure, reporting that ransomware hit 14 out of 16 essential US infrastructure sectors in 2021. Some of the more established among these gangs have shifted their focus in the US from "big-game" organizations to mid-size companies, according to CISA. Additionally, some groups have expanded their partnerships or invested in other groups, combining their expertise to add more capabilities to their current application.

Western countries' decision to disconnect certain Russian banks from SWIFT, the messaging service that connects banks globally, will tie up funds for Russia, making it more challenging to fund Vladimir Putin's war offensive. With hindered ability to move money globally, it could be a matter of time before the Russian government turns to cryptocurrency and ransomware to replenish that currency. Accordingly, it is reasonable to expect an uptick in ransomware attacks in the coming weeks.

Blackbyte a New Concern

The FBI recently released an advisory about BlackByte, the new kid on the block in the ransomware ecosystem. Since emerging last year, joining ransomware-as-a-service (RaaS) operations, BlackByte has compromised the critical infrastructure sectors of government, finance, and food and agriculture. Most recently, the San Francisco 49ers were attacked by BlackByte just before the Super Bowl.

While a previous version of the malware contacted IP addresses to download a .png file with a single symmetric encryption key, a newer version of BlackByte encrypts without communicating to a command-and-control (C&C) server. This eliminates any opportunity for defenders to capture a decryption key that would otherwise be transmitted via network traffic to attackers during the ransomware's encryption process. The lack of C&C communication also makes it more difficult to detect data exfiltration, as data is exported to new servers that are not on the radar of defenders.

Trickbot Under New Management

Malware and botnets come and go. Trickbot, a botnet and banking Trojan that has been lighting fires worldwide since 2016, is the latest to close up shop.

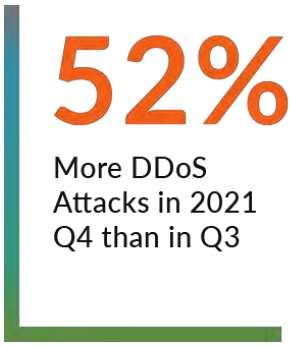
Over time, Trickbot's operations had become harder to keep afloat. Security professionals were more adept at detecting its initial access, conducting takedowns of its C&C servers, and identifying affected organizations. Meanwhile, law enforcement succeeded in arresting some of the individuals behind the malware. Trickbot's relationship with the Conti ransomware group, a gang that has extorted hundreds of millions of dollars from organizations, has now led to its acquisition by Conti. Under Conti's banner, Trickbot's core developers will reportedly focus on BazarBackdoor, a stealthier piece of malware.

The new capabilities the Conti group has acquired as a result of this transition can only support the expansion of its malicious activity. While Conti tends to focus on US and European companies, it recently threatened to hit the critical infrastructure of any country organizing war activities against Russia.

DDoS Rising

DDoS attacks have always been a constant in the threat landscape, usually taking a back seat in the media to other threats such as ransomware. But in recent years, threat actors have begun monetizing these attacks. Attackers leverage botnets such as Mirai to offer DDoS-for-hire services to paying customers or to conduct DDoS extortion, wherein they demand a ransom to abstain from a DDoS attack.

DDoS attacks have become more powerful and debilitating to organizations, and according to reports, they've seen a significant increase of late. Microsoft recently disclosed that in November of last year, it fended off what it calls the largest DDoS attack ever, at 3.47 terabytes per second (Tbps). Q4 2021 also found Cloudflare mitigating the largest DDoS attack it has ever seen, at almost 2 Tbps.



Kaspersky recently noted the number of DDoS attacks in Q4 2021 was 52% higher than in the third quarter and 4.5 times higher than in Q4 of 2020. According to Kaspersky, the drop in cryptocurrency value is one factor, as botnet owners tend to switch from crypto mining to DDoS attacks when cryptocurrency prices fall.

While DDoS attacks are generally seen as less severe than data loss or ransomware, they are still a potent threat. With the capability to slow or completely disrupt the web presence of companies, DDoS attacks are pricey in the downtime they cause, the business and sales they impede, and the potential reputation damage they inflict.

Contact the CBI Threat Intel Group at securityalert@cbisecure.com