Threat Intel Report

Prepared by:

CBI Threat Intel Group

May 19, 2022

A CONVERGE COMPANY

Every enterprise has threat intel sources, detection tools, logging and monitoring capabilities, and other resources that produce data. Data, of course, is mere facts and statistics. In infosec, these statistics may relate to your environment, third-party tools and vendors, or recent or historical cyber attacks.

Last month's report touched on the importance of knowing how and where your organization's data is stored—whether inside or outside your environment. Knowing your data is the first step; after that comes the application of context and analysis. Data may be just facts, but combined with the proper context and analysis, it can drive action.

Threat actors use context, and we saw this recently with the Lapsus$ group. Although the group lacked sophisticated attack techniques, its application of context resulted in several high-profile breaches. These breaches were achieved by carefully analyzing leaked data sets to see what value could be extracted. Lapsus$ might, for example, assess which contractors a data set would give them access to and which companies, in turn, they could access via those contractors.

As security professionals, we too should add context to every piece of data available, whether it's data in our own environments, data from third-party tools and vendors, or data lurking on the deep web. We should use context and analysis to determine which data is valuable, what is vulnerable, and prioritize accordingly. By applying context, we can make informed decisions that help improve our organizational security posture.

Updates

Ukraine

As the war between Russia and Ukraine extends, the security community has grown accustomed to news of cyber attacks between the two forces. Alerts warn us about the possibility of these attacks having a ripple effect on organizations and the possibility of malicious cyber activity against US critical infrastructure.

To date, of course, no major attack has taken place that would fall in the realm of a catastrophic cyber event. Amid the ongoing blitz of information and intel, there is a danger of complacency setting in, during which critical events can be missed. This point was underscored when the NSA's director of cyber security recently asserted that despite the lack of a significant attack, Russia should not be underestimated.

NIST

warns that Russia should not be underestimated in future attacks

As professionals, we must battle complacency by taking in all data, adding context, prioritizing, and remaining vigilant. As this world event continues to unfold, CBI will strive to provide accurate, up-to-date intelligence to help organizations make informed security decisions related to Russia and Ukraine.

Lapsus$

Last month we covered the string of Lapsus$ attacks that ended with the arrest of seven of the group's members. The group's members apparently number more than the seven arrested because the following week, Lapsus$ announced on its public Telegram channel its breach of Globant, a software development firm based in Luxembourg. Since it disclosed the Globant breach, Lapsus$ has been quiet.

Lapsus$ differs from typical ransomware threat actors because it doesn't typically rely on malware. The group buys initial access to organizations by purchasing password lists, VPN access, or compromised accounts from other threat actors. And rather than using crypto malware to lock up files and systems, the group's primary extortion technique is exfiltrating and leaking confidential data.

This technique has proven to be lucrative and repeatable. Journalist Brian Krebs recently reported that, based on his review of leaked internal Lapsus$ chats, the group had also breached T-Mobile multiple times in March before its group members were arrested.

Emerging Threats

Emotet in testing phase

Since the resurgence of Emotet, which we covered in our February report, the malware, once among the most costly and destructive threats, has been manageable with current tools and additional safety measures. For example, Microsoft announced it would begin blocking macros by default for its five Office applications to curb the abuse of macros in phishing by Emotet and other malware families.

However, as usual, attackers always find other ways to get to their victims, and Emotet is no exception. In late April, Proofpoint detailed its observation of a new kind of Emotet activity. The attackers behind Emotet are usually known to blast out tens of thousands of emails delivering either Office attachments or URLs that link to Office files. But in April, attackers began dripping out a low volume of emails distributing Emotet via OneDrive URLs. These links hosted zip files containing Microsoft Excel Add-in (XLL) files. The emails featured one-word subject lines such as "Salary."

The low volume of emails indicates that attackers were likely experimenting with new attack techniques for use in larger campaigns. Similar to marketing departments conducting user testing to measure the responsiveness to an advertisement or product, Emotet, in the wake of Microsoft's new macro blocking policy, was likely doing its own user testing to assess the effectiveness of other techniques and keywords.

CBI researchers reviewed several of the OneDrive URLs and found that each link was associated with a keyword from the email subject lines. But not every URL delivered a payload, leading our analysts to speculate that some of the URLs were instead used to gather metrics about what would entice users to interact the most.

Bumblebee

The development of attack tools has traditionally been driven by the implementation of security controls. As illustrated previously in the case of Emotet, defenders develop a new detective technology or security control, and attackers advance their tools to find ways around these new technologies.

CONTI

Previous TTPs lose their sting, prompting shift to Bumblebee

The case of the new-on-the-block Bumblebee malware appears to stand in contrast to this pattern. Rather than being driven as a response to a defensive technology, Bumblebee appears to have emerged as a result of politics — the Ukraine war in particular.

The story begins when the ransomware group Conti, as reported in our March issue, declared its loyalties to Russia. This stance didn't sit well with one security researcher, believed to be Ukrainian, who protested the gang's support of Russia by leaking more than 60,000 of the group's internal chat messages followed by Conti ransomware source code.

The leaks enabled security companies to write new detections for Conti's development projects, rendering some of their malware ineffective. Because this new strain shares many of the same features and TTPs as other Conti projects such as Trickbot and BazarBackdoor, it is our speculation that Bumblebee has buzzed onto the scene to replace other Conti malware.

In describing the malware, Proofpoint notes that Bumblebee "is a sophisticated downloader containing anti-virtualization checks and a unique implementation of common download capabilities, despite it being so early in the malware's development."

As Bumblebee is new and in the development phase, researchers and security professionals are still identifying indicators. Threat actors that initially utilized BazarBackdoor and BazarLoader have quickly adopted Bumblebee, as have new threat actors. As CBI collects indicators, we will publish them in future SPOT reports.

Benefits of context

According to Oxford Dictionaries, context is "the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed." Threat actors gather information on victims and apply context to define or to meet their objectives. As security professionals, we should also apply context to the data we consume. Using the same context that threat actors are applying may not prevent an incident 100% of the time. Still, it can provide many valuable benefits, such as insights about threat actors, improved IR times, and better communication, planning and investments.

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