KIVU

Threat Intelligence Reports

Cyber threat intelligence insights for claims and underwriting professionals

Vol 23 | March 2020

Purpose
To share cyber threat intelligence and protect digital assets globally.

Sources
This publication incorporates publicly available and proprietary Kivu cyber threat intelligence.

Subscription/ Questions
To receive these reports straight to your inbox, sign up to our mailing list.

Contact us
www.kivuconsulting.com
info@kivuconsulting.com
415.524.7320

Kivu Consulting has offices across the U.S., Canada and in Europe. Click here for our global locations.

How We Expect COVID-19 To Affect Ransomware

Increased attack surface area

It is no secret that threat actors capitalize on holiday weekends and summer vacations, because it is during these periods that they are the least likely to be interrupted as they carry out their attack. The cascade of school closures and empty offices will give ransomware actors an unprecedented landscape of opportunity. Kivu's case metrics show that at least **54% of ransomware attacks we've investigated in 2020 were deployed over the weekend**, up from the **37.5% of attacks** that we responded to in 2019. This increase aligns with the trend of targeted attacks over opportunistic attacks, and elevated sophistication among ransomware distributors. We can expect threat actors to recognize and take advantage of their greater odds.

Risky remote solutions

Companies that will incur the most risk are those that have never supported a remote infrastructure, but are being forced to do so now, with little to no time to enact proper policies and safeguards. We expect to see a dramatic growth in unsecured Remote Desktop Protocol (RDP) traffic, which will be fully visible to cyber criminals monitoring vulnerable nodes. RDP intrusion was the preferred vector of attack for **40-50% of ransomware attacks** we responded to in 2019, leveraged most frequently by the **Dharma, Mamba (DiskCryptor)** and **Phobos** ransomware families. We have every reason to believe that it will continue to be exploited.

While it is an important step to enforce that remote access be conducted using a virtual private network (VPN), companies must also ensure multifactor authentication is mandatory, and monitor their VPN software for known vulnerabilities.

Additionally, we expect companies to face unplanned intermingling of company-owned and personal devices, without a proper Bring Your Own Device (BYOD) policy in place. BYOD guidelines are critical for limiting data exposure and regulating how mobile devices and home devices access company resources, especially when they're not protected by company security systems.

At the same time that we're seeing vulnerable business populations emerge, we're also pondering some positive implications these shifts might have, both for overall resolution of an incident and for thwarting our adversaries.

Impact on Emotet & Trickbot infection rate

With scores of businesses closing and laying off staff, so too comes the closure of company email accounts. Many threat actors rely on the initial careless click by an end user in an enterprise environment to launch a cyber-attack. Will the reduced volume of corporate email targets cause the attack pool for Emotet and Trickbot to shrink? While some threat groups maintain a diversified attack toolkit and exercise multiple approaches for initial entry, groups like **Ryuk** and **BitPaymer** rely almost exclusively on their information-stealing malware partners to

obtain and give them access to their intended victims. Without access to compromised victim networks, some ransomware operations could be out of business, or at the very least on hiatus while they develop a new method for gaining entry. The cybercrime supply chain may be subject to their own set of disruptions linked to COVID-19.

Reduced impact of the "public shaming" approach

Since November, seven ransomware groups (Maze, REvil, DoppelPaymer, Nemty, and reported by Bleeping Computer on 03/24/2020, Nefilim, CLOP, Sekhmet) have adopted the tactic of doxxing to pressure victims of ransomware into paying, even if they have viable backups. This approach involves the theft and publication of the victim's sensitive data in hack forums and on hosted sites. The threat actors promise that the public shaming can be avoided as long as the victim pays. Setting aside the fact that the mere theft of that data by the bad actors may already be a privacy breach (regardless of whether it is published or leaked), small to medium sized companies are facing the looming uncertainty of whether they will be viable in 3-6 months. Such concerns may eclipse the threat of leaked data and fail to have the intended effect on victims.

With less emphasis on operations, incident recovery may be easier

One of the omnipresent challenges of recovering from a cyber incident is balancing network hardening and data preservation without exacerbating business interruption and operational efficiency. Some food for thought: for businesses that will be hit during this time, will recovery efforts be hindered by the absence of onsite resources to direct the workflow, or will recovery turnaround times actually be accelerated, since operations will be at a reduced capacity already, and the organization will be facing less pressure to return to normal production? This undoubtedly will be affected by the industry of the victim, but it's a metric that will be interesting to measure in six months.

Threat Intelligence Reports

Cyber threat intelligence insights for claims and underwriting professionals

Vol 23 | March 2020

About the author

Lizzie is an Associate Director of Cyber Investigations at Kivu Consulting in Washington, DC. Lizzie has over 7 years' experience in legal services, incident response, and digital forensics. She specializes in cyber extortion and threat intelligence with a focus on attacker negotiations, threat actor profiling and data breach remediation. Lizzie's past case work has included network intrusions, e-commerce compromise, business email compromise, employee misconduct, and over 220 cyber extortion investigations.

Contact: Elizabeth Cookson | ecookson@kivuconsulting.com

About Kivu

Kivu is a leading global cyber security firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to cyber-attacks and ransomware incidents. By combining analyst expertise, patented proprietary technology and exclusive threat intelligence, we deliver cutting edge cyber security solutions to organizations in need across the globe. Headquartered in the U.S. with offices worldwide, Kivu is a trusted cyber incident partner to insurance carriers and law firms.