A False Promise of a Pause on Ransomware Attacks in Healthcare

BY LIZZIE COOKSON, MS, EnCE

Associate Director of Cyber Investigations

The internet has been buzzing with reports that ransomware operators promise not to target health and medical organizations during the Coronavirus (Covid-19) pandemic.[1] We know that disruptions to health care organizations caused by ransomware can prove fatal[2], and the risk of an attack during Covid-19 has amplified the danger. It is too early to know whether there is a downtick in attacks; however, we believe ransomware groups are still working with other malware operators in setting the stage for a maelstrom of attacks.

On March 17, 2020 Lawrence Abrams, the creator of Bleeping Computer, contacted ransomware groups, Maze, DoppelPaymer, Ryuk, Sodinokibi/REvil, PwndLocker, and Ako ransomware among others and asked if they would continue targeting health and medical organizations during the outbreak.[3]

Except for Ryuk, most of the groups contacted claimed they would halt attacks against health and medical organizations. CLOP ransomware reportedly denied having ever gone after the likes of hospitals and nursing homes and had no plans to start doing so. DoppelPaymer proclaimed they would decrypt the files for free in the event a healthcare entity inadvertently fell victim to their attacks (but added they will be “triple” checking the identities of victims to ensure no one is trying to weasel out of payment by posturing as such a company).

Additionally, similar discussions are appearing in the underground cybercriminal community and on the dark web. Researchers have recently come across a dark web user who received negative responses from his or her fellow community members after inquiring how to best to exploit Covid-19.[4]

On the surface, this appears reassuring. However, via exclusive threat intelligence feeds, Kivu has seen steady activity from the trojan groups that stage many of the more disruptive attacks.

It is important to understand how targeted ransomware attacks are staged. Before ransomware actors gain access to a system, networks are often first compromised by information-stealing trojans, masquerading as legitimate software. These trojans are typically delivered via phishing campaigns, either through a link in the body of an email or as a weaponized attachment. Once triggered, these trojans perform multiple functions related to network reconnaissance and report the metrics they collect back to the hackers' Command and Control (C&C) servers.

Once access is established, the ransomware groups can acquire the credentials to launch an attack. From the list of thousands of compromised networks, those perceived as high value are then put on a short list to be targeted for ransomware. It is extremely important to note, however, that there is no definitive or consistent timeline between when the trojan infection is introduced and when the ransomware attack begins. In Kivu's experience, the period of dormancy between trojan and ransomware can be as long as 12 months, as short as 24 hours, or anything in between. The human-operated nature of big game ransomware allows the bad actors to decide precisely when they wish to detonate the attack.

While ransomware groups may claim to adhere to a moral code in avoiding attacks on the healthcare sector during this time, that does not extend or have bearing on the intentions or actions of their malware partners. We believe it is likely that pre-attack trojan infections will persist at their usual rate among healthcare and all industries alike, and ransomware operators will either (a) attack at will, like some continue to do[5], or (b) patiently sit on their treasure chest of kingdom keys that continue to be harvested until the global effects of the pandemic begin to subside and scrutiny on healthcare attacks starts to diminish. Even ransomware groups value good press and will take the opportunity to perpetuate the illusion that they are amongst the honorable contingent of thieves.

It is crucial to understand that if your organization is not suffering an active extortion attack, there is still every possibility that the groundwork is quietly being laid for a future ambush.

Unlike some malicious files that have static signatures and run from a single location, trojans like Emotet and Trickbot are polymorphic in nature. Each new copy of the trojan is not only designed to have a new signature, but to download under a different filename, and live in multiple unique directories. Signature-based detection only recognizes a malicious file if that file's signature has previously been reported as harmful. Emotet and Trickbot churn out unique signatures nearly every time they replicate, making it effectively impossible for traditional antivirus to keep up with each iteration. The only solution that can combat this kind of threat is detection based on behavior and heuristics, which can detect, isolate, and kill files that are behaving abnormally, even if they have an unknown signature. There are many endpoint monitoring solutions available that use behavior-based detection to thwart trojan infections.

Aside from deploying a robust endpoint monitoring and detection (EDR) agent, other methods that can identify the presence of a trojan infection include:

- Reviewing antivirus logs for Emotet, Trickbot or other trojan alerts in the last 30 days (or longer, depending on your retention policy).
- Reviewing PowerShell logs for suspicious and/or encoded activity.
- Checking the **%appdata\local\temp%** and **%appdata\roaming%** directories for suspicious files and folders you do not recognize.
- Checking for scheduled tasks you do not recognize. Some trojans will automatically create tasks upon execution to maintain persistence.
- Asking employees if they recently clicked on any **links** or **attachments** in emails pertaining to invoices, payroll, receipts, or Covid-19 related guidance.
- Reviewing traffic logs for anything communicating over port 445, 447, or 449 (these ports aren't inherently malicious, but they are favored by trojans).

[1] https://securityboulevard.com/2020/03/maze-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid-19-outbreak-but-how-trustworthy-is-their-word/

[2] https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks

[3] https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

[4] https://www.digitalshadows.com/

[5] https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#42efaffa18e5

Incident Response Services

Kivu's forensic investigators are experienced in cases involving compromise of data, theft of trade secrets and unauthorized access to data. Our qualifications include forensic certifications (Encase Certified - EnCE, SANS GCIH Incident Handlers, Certified Ethical Hackers, and reverse malware experts); IT certifications (Certified Information Systems Security Professional CISSP and Certified Information Systems Auditor CISA); and prior backgrounds as legal counsel, IT administration, law enforcement, and network security. Kivu investigators have testified as computer forensic experts and have presented their findings to US and UK regulators..

Post-Breach Remediation Services

Kivu provides fast and effective on-site technical remediation assistance to restore our clients' IT networks and recover data and operations following ransomware and other malware attacks. Kivu's services include hardening systems and implementing improvements to network security.

Enterprise Protection Services

Kivu leverages its incident response experience to also offer services that proactively address cyber risk and improve security before an incident. Kivu's services include Managed Endpoint Detection and Response, Vulnerability Scans, Penetration Tests, Risk Assessments, Security Program Reviews and Virtual CISO/Architect Staff Augmentation services.

About Kivu

Kivu is a global technology and cyber security services firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to data breaches and proactive IT security compliance. Headquartered in the U.S. with offices worldwide, Kivu is a pre-approved cyber forensics partner for leading North American and EMEA insurance carriers.

kivuconsulting.com

KIVU EUROPE

51 Eastcheap
London, EC3M 1JP
info@kivuconsulting.com

OUR GLOBAL OFFICES

kivuconsulting.com/locations