Kivu

Threat Intelligence

Subject: Ransomware – 2018 Year in Review

Date: January 14, 2019

Lizzie Cookson, Associate Director, Kivu Consulting

Kivu investigated more than triple the number of ransomware incidents in 2018 that we did in 2017. Unlike the predictable ebb and flow of the 2017 attack landscape, 2018 was a year of surprises. Attack vectors became varied, reconnaissance efforts ramped up, a new age of actors entered the cybercrime arena and the impact of cyber-attacks seemed to last longer and with more devastating effects.

Coming into 2018, *SamSam* was one of several ransomware groups we considered kingpins of the extortion game, but by the end of the year, their attack incidence seemed to have slowed, their mechanisms became disorganized, and on November 28, 2018, the U.S. Department of Justice announced indictments of two Iranian *SamSam* ransomware operators who are alleged to have collected over $6 million in ransom funds across 200+ victims since 2015. *SamSam* has fallen relatively silent since the announcement.
With the fall of *SamSam* came the rise of two new ransomware variants, arguably more vicious, more destructive, and stealthier than all of their ransomware peers: *BitPaymer* and *RYUK*.

Shift in Threat Trends:

The introduction of *BitPaymer* and *RYUK* signaled several important shifts in the extortion landscape:

(1) Unlike competing ransomware strains who charge flat fees or notably low fees (i.e. 0.5 BTC, 1 BTC, $5,000 worth of BTC, etc.), these groups charge sums in the hundreds of thousands and even in the millions. How do they justify these outlandish sums? By doing their homework. *BitPaymer* and *RYUK* actors perform days, weeks or even months of reconnaissance prior to the attack and come to the negotiating table armed with a specific set of metrics about each victim. They are able to cite company identity, yearly revenue, employee count, and size of the environment (server and workstation count). When the attacker has so much visibility into the victim's identity, price negotiation becomes less feasible the likelihood of paying the full sum is high.

(2) An overwhelming majority of our *BitPaymer* and *RYUK* victims reported a simultaneous banking trojan infection at the same time they discovered the ransomware attack. This is a stark departure from years past when it was highly anomalous for ransomware to come bundled with any additional threat. Our ensuing investigations into these matters revealed what we believe is a collaborative effort between banking trojan operators and ransomware operators to

exploit a single victim multiple times for different ends. The banking trojan actors collect banking information along with network metrics, email passwords and stored credentials, and share/sell the extraneous (yet valuable) information to other cybercriminals who wish to pursue different ventures (like extortion).

This sinister era of criminal collaboration and tailored exploitation of a single victim has resulted in organizations suffering significant business disruption, long-term compromise, and the pressing need to implement greater hardware and software defenses to combat multiple threats. When ransomware was more random/opportunistic, it was much easier to mitigate and move on (i.e. close your Remote Desktop Protocol (RDP) port and change your passwords).

BitPaymer, RYUK, RaaS:

Another trend that exacerbated claims last year was the increase in "bad" ransomware strains that cause significant file corruption and/or are operated by extremely unskilled actors who cannot resolve issues that more seasoned programmers normally could help with.

The issues with *RYUK* (and to some degree *BitPaymer*) start with the destructive wake of the encryption scheme. Well-designed decryption tools (e.g., *GandCrab*, *SamSam*) should swiftly decrypt files with very few issues related to corruption, skipped files, or system failures. With *RYUK* and *BitPaymer*, we encountered persistent, mammoth-sized obstacles with decryption, including:

- Timeline to decrypt most environments is weeks rather than days, extending business interruption time
- Buggy tools that constantly pause/quit, requiring scripts to circumvent the issues OR round-the-clock boots on the ground to prompt continuation of the tool
- Deliberate vandalization of client environments, such as formatting entire drives, disabling admin privileges on IT accounts, destroying Citrix environments, etc. (seen with *RYUK* only)
- On occasion, complete and total failure of the tool and zero assistance from the attacker (seen with *RYUK* only)

The other groups responsible for less-than-smooth recovery are those that use Ransomware-as-a-Service (RaaS) platforms, which spiked in popularity in 2018. Note: RaaS is not always synonymous with bad; *GandCrab* is a great example of a skilled threat group that uses RaaS distribution, but tightly controls their pool of operators to include only other actors who have vetted hacking skills. Unfortunately, most RaaS platforms seem to have no screening process and allow access to their ransomware to anyone with a pulse.

Many of the RaaS actors we came in contact with in 2018 were volatile, incompetent, and unpredictable. We had actors who provided bad tools, incomplete decryption keys, actors who lost track of keys, actors who charged us 2-3x because they forgot we already paid and refused to acknowledge their error, actors who dropped off the face of the earth for weeks, or sometimes permanently, leaving the victim with no means to restore…the list goes on. Because more rookie extortionists have entered the market, the challenges of resolving a ransomware attack have intensified. This is why having responders with in-depth knowledge of variants and threat actors is more crucial now than it's ever been.

As ransomware moves towards greater sophistication in propagation (number of machines hit) and attack vector (method of gaining access to the network), resources required to mitigate the attack multiply:

- **Propagation**. Because *BitPaymer* and *RYUK* have attack mechanisms that can cripple multiple sites for a single organization in a short amount of time, the need for boots-on-the-ground resources is greater. Because we anticipate more system failures and environment destruction with these variants, troubleshooting and rebuilding needs are becoming the rule rather than the exception.

- **Banking Trojans**. Previously, ransomware would rarely cause so many issues; it was just a matter of buying the tool, unlocking the files and putting everything back online within a few days because it was extremely rare that any residual threats were present on the machines post-decryption. With *BitPaymer* and *RYUK*, mitigating the ransomware issue does nothing to solve the banking trojan problem, which means even after they decrypt, they can't go back online without putting themselves at risk. So, what can they do? Remove the trojan? Not so simple. Banking trojans are polymorphic in nature and fiercely resistant to most signature-based antivirus solutions; they constantly replicate to random locations and rename themselves under dynamic filenames, so even if you run multiple AV's over and over and manually try to remove files, you're not going to find them all. Because "cleaning" banking trojans is an impossible endeavor (as opined by the Department of Homeland Security), the organization is faced with the daunting task of total hardware replacement if they (a) want to make sure the threat is really gone and (b) don't want to destroy evidence and open themselves up to litigation down the line. For a company with 400+ servers, thousands of workstations, in multiple locations, potentially in multiple countries, this is a long, painful, expensive journey.

- **Attack vectors**. 2017 was the year of brute force RDP intrusion. It was the preferred vector for most variants, and from a security standpoint, a very simple vulnerability to close. In 2018, Kivu still observed the use of RDP intrusion, but also saw phishing make a comeback (and not in the traditional way), a rise in exploit kits, and malicious software downloads. Stealthier attack vectors (i.e.

social engineering + credential harvesting + exploit kits) leave fewer footprints and are thus much harder to confidently prevent. As attackers rely less on noisy, easily-detected-and-eliminated entry points and move towards sneakier entry methods, victims who previously have not met the definition for low-hanging fruit may now become at risk and the costs to resolve those vulnerabilities will be higher. For example, closing an RDP port requires little time/effort, but patching operating systems in a 1200-device environment, or retiring a Windows 2003 server that runs legacy software necessary for operations is something that cannot happen overnight and may require the assistance of outside vendors.

Lizzie Cookson is an Associate Director at Kivu Consulting in Washington, DC. She specializes in data breach response and ransomware, including attacker negotiations and payments, remediation, and threat hunting. Lizzie's case work has included malware infections, network intrusions, data breaches, intellectual property theft, employee malfeasance, and over 100 ransomware investigations.

Lizzie has 8 years' experience in legal services and cyber investigations. Prior to joining Kivu, she worked in regulatory roles at law firms in Massachusetts and Washington, DC while earning her graduate degree in digital forensics.

About Kivu

Kivu's data security experts and forensic investigators are experienced in protecting organizations against compromise of data, theft of trade secrets and unauthorized access to personally identifiable information. You can count on our real world investigative experience to provide cutting edge data security advice on issues we are seeing in the field right now. Our qualifications include IT certifications; Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and various forensic certifications including; Encase Certified (EnCE), SANS/GIAC Certified Incident Handler (GCIH), Certified Ethical Hackers, and reverse malware experts. Our experts have prior backgrounds as network security professionals, IT administrators and legal counsel.

Kivu's investigators have testified as computer forensic experts in US state and Federal courts, and presented their findings to US and EU regulators.

More information about Kivu can be found at www.kivuconsulting.com.