Enterprise Malware-as-a-Service: Lazarus Group and the Evolution of Ransomware

In an interesting twist to the use of ransomware, an attacker leveraged a vulnerability in a plug-in for a remote-monitoring tool, Kaseya VSA, to gain access to a small Managed Services Provider, and infect approximately 80 companies with the GandCrab ransomware. This is a notable shift in tactics for purveyors of ransomware, and follows the trend of commercial crimeware being used to attack businesses, and now service providers, rather than individual.

The History of Ransomware: From Userspace to the Enterprise

The history of ransomware (extortion via malicious software) goes all the way back to 1989, with PC Cyborg, also known as the AIDS Trojan, written by Joseph Popp. The malware had serious flaws, allowing key extraction from the code itself, and ultimately did little damage in comparison to the most destructive attacks to date, WannaCry and Petya/NotPetya. The first robust ransomware emerged with the introduction of public-key-cryptography to the ransomware concept by Adam L. Young and Moti Yung. Young & Young's experimental malware, and coined the term cryptovirology, encompassing overt and covert attacks utilizing cryptographic functions. By 2006, various ransomwares had begun to utilize more sophisticated RSA encryption schemes and larger key sizes. In 2008, the malware known as Gpcode.AK utilized a 1024-bit RSA key, which was determined to be computationally infeasible to break without a distributed effort.

In 2013, the now infamous Cryptolocker ransomware netted its operators an estimated $27 million from infected users, shooting ransomware to the top of the profitable e-crimes list next to banking trojans. Cryptolocker itself evolved, and soon began targeting network-attached storage devices, and in 2015, began to target Linux-based webservers. Further evolution of ransomware came with CryptoWall, which utlized a digital signature in an effort to appear trustworthy. CryptoWall took further destructive measures as well, deleting volume shadow copies, on top of its capabilities of password-stealing and BitCoin wallet hijacking. The SamSam ransomware, which was first detected in 2016, targeted JBoss servers. Rather than utilizing email phishing and malicious documents, SamSam directly infected webservers over the internet. Victims of SamSam included hospitals, and local governmental bodies in the United States: the city of Atlanta, GA, USA, was completely crippled by SamSam in March 2018.

In May 2017, the highly destructive WannaCry ransomware spread across the internet using an exploit named EternalBlue which was leaked from the U.S. National Security Agency. An estimated 230,000 systems were infected in more than 150 countries. The malicious

software demanded money from users in 20 different languages. WannaCry was the first ransomware to affect enterprise organizations, which included Telefónica, the British National Health Service, FedEx, Deutsche Bahn, Honda, Renault, and even the Russian Interior Ministry. For the first time, the global enterprise was forced to deal with threats which were unconcerned with stealing trade secrets, but instead acted to cause as much destructive damage as possible if their demands were not met.

In March 2018, the Petya ransomware made its first introduction, followed by a heavily modified version which wreaked havoc on business, most notably the logistics firm Maersk, whose Business IT infrastructure was almost completely destroyed, and terminals in four countries were impacted, causing delays and disruptions for weeks. Speculation from industry experts, including noted exploit developer known by his handle, the grugq noted that NotPetya's purpose appeared to be wholly destructive, and without concern for collecting extortion fees, as is the general operation of file-locking malware. Instead, NotPetya simply performed permanently destructive acts on the systems it infected.

Nation-State Cyber-Attacks as a Service

A ransomware known as HERMES began appearing in October 2017, when it was used against an attack against the Far Eastern International Bank in Taiwan. $60 million was stolen in a sophisticated attack on the SWIFT system. Notably, the HERMES ransomware appeared to be used solely as a diversion from the true heist: the attack on the SWIFT system. Almost one year later, in August of 2018, a new type of ransomware infection burst onto the stage: Named Ryuk, after the name with which the ransom notes were signed, victims included large newspaper publications such as the New York Times, Los Angeles Times, and Wall Street Journal.

HERMES was attributed to the infamous Lazarous Group, believed to be funded by the government of North Korea. As samples of Ryuk were analyzed, it was found to re-use code from HERMES: a solid link to Lazarus Group. Ryuk is a fully-developed ransomware package, and unlike HERMES, is not a decoy: the malware is wholly intended for the task of digital extortion. Ryuk marks the third time that Lazarus Group has used destructive malware against its targets, the most notable being Sony Pictures in 2015, where ransomware was used to destroy studio infrastructure.

Dominating ransomware news recently has been the ransomware-as-a-service GandCrab: the software is maintained by a dedicated development team, whom deliver frequent updates with additional capabilities and evasion techniques. Continuing with the trend of organized crimeware targeting businesses instead of end-users, GandCrab was used to infect the customers of a small Managed Services Provider, by way of breaching the MSP itself. Rather than the MSP, the customers bore the infection and potential costs of ransom. By targeting the MSP, the attackers managed to infect 80 victims at the same time. Practical and efficient.

Opinion: Lazarus Group and the Evolving Landscape of Enterprise-capable Malware

The trend of crimeware shifting from targeting end-users to targeting the enterprise has continued in other malware areas, specifically with the evolution of the Emotet malware, a trojan which targets bank information. First identified by researchers in 2014, it has evolved from a simple money-stealing trojan which spreads via malspam campaigns, to a sophisticated malware toolkit capable of stealing emails and spreading via the infamous EternalBlue exploit. Emotet is now capable of infecting an entire organization via its lateral movement capabilities.

The line between organized crimeware and nation-state espionage-ware is a fine one indeed: in a report by Cybereason's Intelligence Unit released in February 2017 at the RSA Conference, Russia, China, and the United Arab Emirates have been found to be outsourcing targeted operations to dedicated hacking groups, presumably in further attempts to mitigate risk and foil attribution. The use of outsourced labor, and potentially also malware-as-a-service is consistent with changing tactics, techniques, and procedures to confuse and counter one's adversaries. From a purely objective standpoint, these behaviours should be expected.

Lazarus Group has demonstrated a concentrated and continuous effort to develop and deliver both HERMES and Ryuk in targeted attacks, and like other skilled actors, makes efforts to incorporate new evasion, privilege escalation, and lateral movement techniques into new releases. Attribution in malware analysis is frequently difficult (and sometimes impossible), due to a combination of obfuscation techniques, and intentionally misleading clues left by the authors for analysts who stumble upon them, in addition to the copycat nature of crimeware: where one software leads, others will follow, and this path leads straight to improvement and innovation. The authors of crimeware learn from each other's implementations, and from the analysis performed by incident responders.

It is possible, and even likely, that Lazarus Group may manage to breach a large hosting provider, and deliver ransomware to every customer. Such an attack is not only likely, but also fits within Lazarus Group's modus operandi: an attack which infects dozens or hundreds of customers may also effectively obfuscate their true purpose, in the same way HERMES was used to mask SWIFT fraud. McAfee Labs makes similar observations, finding that Ryuk (and by extension Lazarus Group) pose an existential risk to IT Hosting and Freight / Logistics firms.

In the sport of malware-as-a-moneymaking-mechanism, Lazarus Group is a world-class player, and will certainly continue its trend of constantly evolving tactics and targets.

Who we are

The Threat Intelligence -Team helps clients to reduce the threat posed by adversaries to their networks by leveraging the power of collaborative defense in combination with comprehensive analytics and contextualized threat intelligence. DCSO delivers actionable intelligence on all levels – from atomic Indicators of Compromise (IoC) to insights into the political, economic and cultural context of adversaries.