Targeted Ransomware: Proliferating Menace Threatens Organizations

POSTED: 18 JUL, 2019  |  7 MIN READ  |  THREAT INTELLIGENCE

Targeted Ransomware: Proliferating Menace Threatens Organizations
With several new targeted ransomware groups emerging over the past two years, the number of organizations being hit by targeted ransomware attacks has multiplied.

Targeted ransomware has quickly become one of the most dangerous cyber crime threats facing organizations. Over the past two years, the number of organizations being hit with targeted ransomware attacks has multiplied as the number of gangs carrying out these attacks has proliferated.

A successful targeted ransomware attack can be devasting for an organization. Attackers generally attempt to encrypt as many machines as possible, targeting servers as well as ordinary computers, and will often try to encrypt or destroy back up data. The affected organization could have its operations severely disrupted, losing access to vital data and services. Loss of business and reputational damage could add to the likely high financial cost of any clean-up operation.

Faced with this kind of chaos, it is hardly surprising that some stricken organizations consider paying the often-exorbitant ransom demand. Given this outcome, nor is it surprising that a growing number of cyber criminals are turning their attention to targeted ransomware.

In a new white paper, published today, Symantec has found that the number of organizations being attacked by targeted ransomware has grown rapidly since the beginning of 2018.
Multiplying threats

The rapid growth in attacks coincides with the emergence of a number of new targeted ransomware gangs. For some time, the only attacker of note was the SamSam group (Ransom.SamSam), which was responsible for attacks against a string of organizations, mainly in the U.S. However, SamSam’s success meant that it was only a matter of time before other groups moved into this niche. In early 2018, another actor—Ryuk (Ransom.Hermes)—appeared and almost immediately began attacking more organizations per month than SamSam.

By the beginning of 2019, the number of targeted ransomware operations began to multiply, with several more gangs appearing on the scene, including GoGalocker (aka LockerGoga) (Ransom.GoGalocker), MegaCortex (Ransom.MegaCortex), and RobbinHood (Ransom.Robbinhood). In addition to the groups involved exclusively in targeted attacks, there are also a number of ransomware groups, such GandCrab (Ransom.GandCrab) and Crysis (aka Dharma) (Ransom.Crysis),
who've been reportedly carrying out targeted attacks into addition to indiscriminate attacks.

"Number of organizations being hit by targeted ransomware attacks has multiplied in the past year. https://symc.ly/2LmWrEd"

Figure. Number of organizations affected by targeted ransomware attacks, by family, January 2017 to May 2019 (stacked column)

New breed of threat

First appearing in January 2019, GoGalocker typifies the current type of targeted ransomware attack being deployed against businesses. The attackers behind the ransomware are skilled and knowledgeable enough to penetrate the victim's network, deploy a range of tools to move across and map the network while using a variety of techniques to evade detection, before simultaneously encrypting as
many machines as possible.

GoGalocker deploys a number of detection evasion techniques during its attacks, such as digitally signing the ransomware with legitimate certificates, making it far less likely that they will be flagged as untrustworthy.

In carrying out its attacks, GoGalocker borrows many of the tools and techniques used by espionage groups, making extensive use of publicly available hacking tools and living off the land tactics. Once inside the victim’s network, the attackers run PowerShell commands to run shellcode that enables them to connect to the attacker’s command and control server. A variety of tools are then deployed to traverse the network and steal credentials:

- **PuTTY**: a command-line utility used to create SSH sessions.
- **Mimikatz** ([Hacktool.Mimikatz](https://www.symantec.com)): a freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext depending on the configuration.
- **Wolf-x-full**: A multi-purpose tool capable of querying a range of remote machines for basic information, viewing a list of installed programs, uninstalling programs, disabling Windows User Account Control (UAC) and UAC remote restrictions, and disabling the Window Firewall.
GoGalocker deploys a number of detection evasion techniques during its attacks, such as digitally signing the ransomware with legitimate certificates, making it far less likely that they will be flagged as untrustworthy. The attackers will also usually attempt to disable any security software before installing the ransomware. This is not because of any innate weakness or vulnerability in the security software it disables, rather that the group uses stolen administrator credentials to turn the software off or uninstall it.

In several of the attacks seen by Symantec, once the attackers were finished mapping the network, they used batch files to spread the ransomware to multiple computers before executing the encryption process.

As a final precaution, the attackers log off the current user. In at least one case, they also changed local user and administrator passwords using a net.exe command. The likely motive for this was to prevent anyone from logging in and halting the encryption process.

Since first emerging at the beginning of 2019, GoGalocker has already attacked organizations across a broad range of industry sectors including computer services, accountancy and auditing, consultancy, financial services, power tools, building and construction, financial services, publishing, printing, metals, and warehousing and storage. Twenty-three percent of the target organizations were located in the U.S., but outside of this, a high proportion of victims were in Scandinavia, including Finland (23 percent), Norway (15 percent), and Sweden (8 percent).

**MegaCortex link?**

One of the most interesting findings to emerge from the research was the
discovery of some connections between GoGalocker and MegaCortex. Both ransomware families perform the following actions:

- Create a log file in C:\
- Work using the master/slave model
- Use module interprocess in Boost library to share data and communicate between master and slave
- Use functions to enumerate logical drives before encryption
- Use native functions to work with target files:
  - NtOpenFile, NtReadFile, NtWriteFile, NtClose
- Encrypt files using AES-128-CTR
- Execute the command “cipher.exe /w” to wipe unused data after finishing encryption process

In addition to this, the rich header of the MegaCortex and GoGalocker executables is compiled with almost the same version of Visual Studio 2017 (minor build version 27030 and minor build version 27027 respectively). Finally, both ransomware families have used Cobalt Strike malware in their attacks. One of the Cobalt Strike beacons used in a MegaCortex attack connects to an IP address that has previously been linked to GoGalocker.

While it may be possible that both MegaCortex and GoGalocker are operated by the same group, the activity during the pre-infection process points towards distinct groups. A more likely explanation for the link is that both ransomware families were developed by the same third-party developer for two separate groups of attackers.

**Robust defenses needed**

A ransomware attack that involves encryption of hundreds of computers and
servers is probably one of the most disruptive and costly forms of cyber attack any organization could experience. The hastening pace of targeted ransomware attacks over the past 12 months means that organizations need to educate themselves about this threat and ensure that robust, overlapping defenses are in place. The perceived success of the current crop of targeted ransomware groups makes it highly likely that more cyber crime actors will attempt to move into this space.

**Protection**

Symantec has the following protection in place to protect customers against these attacks:

**File-based protection**

- Hacktool.Mimikatz
- Ransom.Crysis
- Ransom.GandCrab
- Ransom.GoGalocker
- Ransom.Hermes
- Ransom.MegaCortex
- Ransom.Robbinhood
- Ransom.SamSam

**Mitigation**

Symantec recommends users observe the following best practices to protect against targeted ransomware attacks:
Local Environment

- Ensure you have the latest version of PowerShell and you have logging enabled.

- **Restrict access to RDP Services:** Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication.

- **Use File Server Resource Manager (FSRM) to lock out the ability to write known ransomware extensions on file shares where user write access is required.**

- **Create a plan to consider notification of outside parties.** In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place.

- **Create a “jump bag” with hard copies and archived soft copies of all critical administrative information.** In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted.

- **Implement proper audit and control of administrative account usage.** You could also implement one-time credentials for administrative work to help prevent theft and usage of admin credentials.

- **Create profiles of usage for admin tools:** Many of these tools are used by attackers to move laterally undetected through a network. A user account that has a history of running as admin using psinfo/psexec on a small number of systems is probably fine, but a service account running psinfo/psexec on all systems is suspicious.

Email
- **Enable 2FA** to prevent compromise of credentials during phishing attacks.

- **Harden security architecture around email systems** to minimize amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.

**Backup**

- **Implement offsite storage of backup copies.** Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.

- **Implement offline backups that are onsite.** Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware.

- **Verify and test your server-level backup solution.** This should already be part of your Disaster Recovery process.

- **Secure the file-level permissions** for backups and backup databases. Don’t let your backups get encrypted.

- **Test restore capability.** Ensure restore capabilities support the needs of the business.

**Further reading**

To learn more about targeted ransomware, download our whitepaper - **Targeted Ransomware: An ISTR Special Report**
About the Author

Symantec Security Response
Security Response Team

Symantec's Security Response organization develops and deploys new security content to Symantec customers. Our team of global threat analysts operate 24x7 to track developments on the threat landscape and protect Symantec customers.
The Revival and Rise of Email Extortion Scams

BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly