Meeting a Russian Ransomware Cell

Published: 2019-11-12 · Archived: 2026-04-05 13:57:27 UTC

Ransomware is one of the most notorious and effective types of cyberattacks in the last decade. And I had the opportunity to go inside the minds that operate a real-world ransomware cell.

It starts with the young leader — nicknamed “Twig” — of a Russian ransomware cell. After two weeks of chatting through a secure channel, what I found was very interesting.

On social media, some cybersecurity firms like to portray him in black hoodies with leather gloves and a backdrop of matrix-style digits. They namedrop buzzwords like advanced-generation V attacks and other trumped up terms, which could be more fitting for nation-state attacks, but this isn’t the case with most hacking groups.

Carrying out successful ransomware attacks typically only requires a mixture of scripts, common vulnerabilities, brute-force efforts, bad IT policies at target organizations, and generations of frustration between eastern and western politics.

On-Demand Webinar: My Two-Week Conversation with a Ransomware Cell

Join SonicWall security expert Brook Chelmo as he gives you an inside look into the human-side of a modern ransomware cell, their advice on how to stop them from infiltrating your organization, encrypting your endpoints, and spreading to other drives and segments of your network.

WATCH NOW

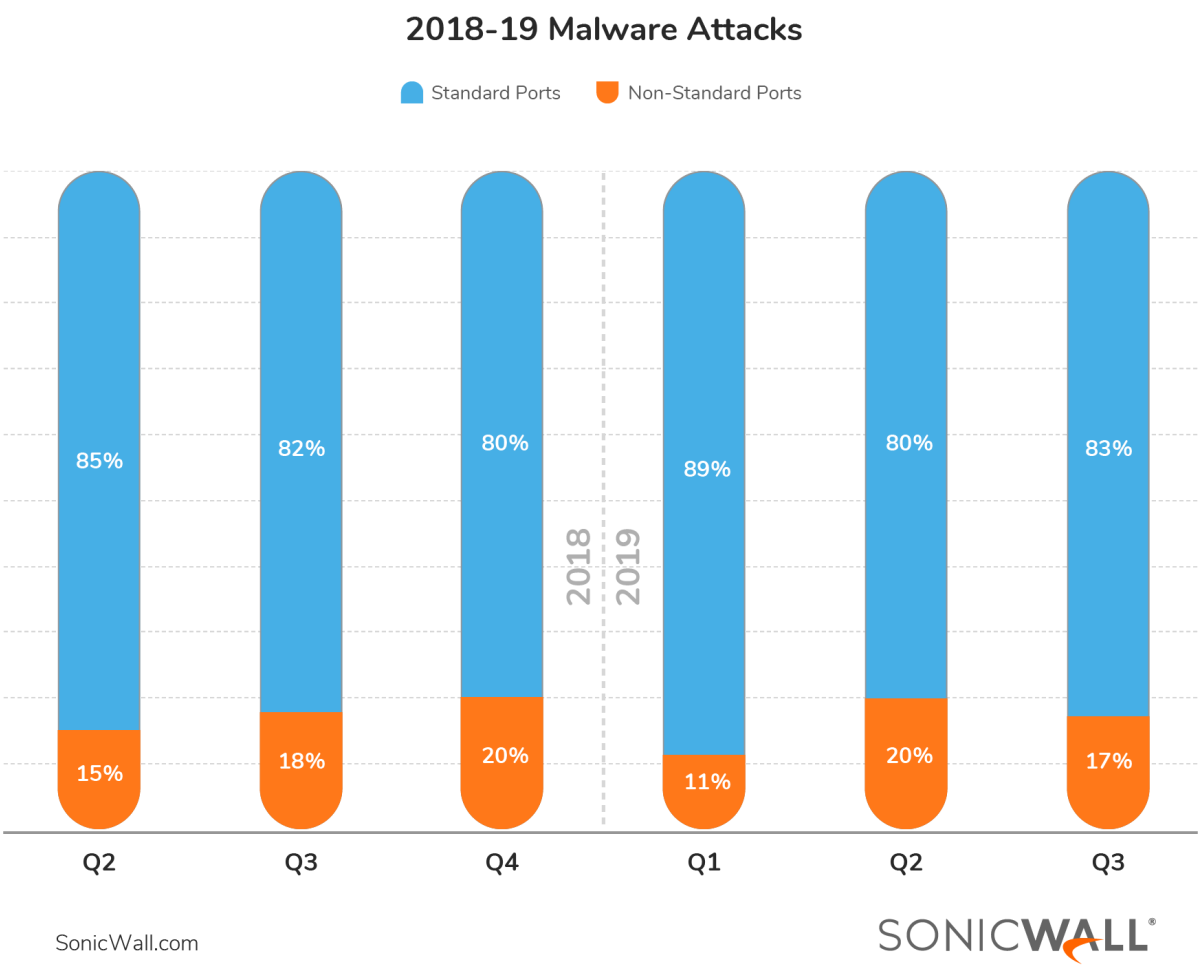
How does a ransomware attack work?

The number of organizations and verticals targeted each week, including the demands they make on the compromised device(s), are all private. Twig, however, is open to saying that their attack style is generally through spear-fishing and port-scanning for common vulnerabilities.

Twig’s favorite ports are “5900 and 5901 which are open and unpassworded.” Together, these two ports rank as the 19th most scanned port. These ports are used by virtual network computing (VNC) for desktop-sharing and remote-control application for Linux and Windows machines.

Over the years, several vulnerabilities related to these ports have allowed attackers to bypass authentication and gain access to the system. If Twig can get in, then your participation isn’t even required to activate the ransomware script (e.g., enable macros on a malicious Word document received in email). In fact, SonicWall

research shows that anywhere between 17% and 20% of all malware attacks come through non-standard ports.



While Twigs scripts are pinging a range of IP addresses for vulnerabilities, he runs a PHP script alongside unnamed services that spam targets to gain remote access to their systems.

HILDACRYPT, for example, uses file extensions that are not normally scanned, such as *.vbox*, to evade inspection and detection by firewalls or email security services. Once access has been granted, he will log in after-hours and run a batch file through PsExec throughout the entire network to make it "go boom."

Or, in less dramatic words, to "make Hilda run on the entire network." It's the same headache caused by the likes of WannaCry, NotPetya and SamSam ransomware strands, the infamous attack wave from three years ago. Since admins tend to have access to multiple drives — and sometimes read/write ability on endpoints via access manager roles — exploiting them is critical to mission success.

> "If Twig can get in, then your participation isn't even required to activate the ransomware script."

Once systems are compromised, they don't exfiltrate the files and sell the data like some do. They just set the demand and wait.

Initially, they asked victims to watch the Hilda series on Netflix (yes, really), join their Discord server for support, then pay the stated ransom amount in bitcoin (a popular way to couch the demand).

What can you do to stop ransomware attacks?

First of all, Twig says to "use proper passwords" for ransomware protection. He said many passwords are either written by the 'crazy or the lazy.' Most of them are too simple and are often guessed by his scripts. His favorite story was when he found a password to be two quotation marks. I guess the administrator thought it was too simple to guess. Well, he was wrong and had to pay for it.

Second, he said "write your programs in a real programing language." He said that real programmers write in *C* or *C++*, and that *Java* or *PHP* is for the lazy and stupid (an opinion not shared by all professional programmers).

When he sees programs written in *Java*, he feels he is dealing with a non-qualified individual and, therefore, an easy target. It is also worth noting that some security professionals advise not to program in *C* when it comes to security.

Third, he casts shade on Americans and tech workers over the age of 35 either because of his belief in their lack of modern skills or energy to do the job properly. He says organizations should hire qualified people who can both code and understand security. If he was in charge of hiring at your company, and didn't discriminate by age or nationality, he would hire people who hold qualifications in *C* or *C++* and have the energy to follow security best practices.

Misconfigured firewalls leave doors open for ransomware attacks

Finally, Twig points out that misconfigured firewalls are his best friend. In fact, he has strong opinions for some firewall makers that enable him "to uninstall from the computer." In the case of network firewalls, misconfigurations are easily done and can be one's downfall. It happens more than you think.

In the case of endpoint firewalls, end-users should be under the principle of least privilege (POLP), which means they will have just enough rights to do their job and without the ability to modify their endpoints. In 2016, Microsoft reported that 94% of critical vulnerabilities can be mitigated by removing administrative rights from users.

Four ways SonicWall stops ransomware attacks

Stopping ransomware attacks isn't always easy. A conversation with Twig makes that apparent. But he also highlights that if you follow best practices and implement security across different layers, ransomware attacks won't be nearly as successful. Leverage the four key ways SonicWall helps organizations block ransomware attacks — automatically and in real time.

- **Deploy a firewall and keep security services active.** Firewall vendors like SonicWall are now security platform providers that protect the traffic to and from branches (SD-WAN), and examine traffic through the firewall with gateway antivirus to stop known versions of malware. It's also smart to leverage Intrusion Prevention Services (IPS) to identify known communication patterns within malware and stop what it wants to do, like travel laterally to other drives or networks. The combination of gateway security and IPS was critical in stopping WannaCry ransomware attacks for SonicWall customers on Day 1.
- **Block unknown ransomware with a sandbox**. However, all of the updated versions of the strain that came after Version 1 were blocked automatically by the Capture Advanced Threat Protection (ATP) sandbox (if the other ransomware variants were found by a customer before SonicWall could create a definition/signature to block it on firewalls and email security).
- **Protect your inbox.** To make it even more difficult to attack your network or users, use secure email solutions to block spoofed emails and examine attachments within all email to look for malware. Email is still highly effective at getting malware exploits onto your network.
- **Secure your endpoints.** Finally, protect your endpoints with a next-generation anti-virus (NGAV) For example, Capture Client will help stop intrusions and ransomware attacks from initiating. Even if a ransomware strain did execute, Capture Client would give the administrator the ability to roll back the damage to a previously known clean state.

For the full story on my chats with Twig, I urge you to attend my upcoming webinar, "Mindhunter: My Two-Week Conversation with a Ransomware Cell."
