Ransomware-as-a-service: The pandemic within a pandemic

intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer

Ransomware is a massive problem. But you already knew that.

Technical novices, along with seasoned cybersecurity professionals, have witnessed over the past year a slew of ransomware events that have devastated enterprises around the world. Even those outside of cybersecurity are now familiar with the concept: criminals behind a keyboard have found a way into an organization's system, prevented anyone from actually using it by locking it up, and won't let anyone resume normal activity until the organization pays a hefty fee.

As economies around the world teeter on the edge of disaster as a result of the COVID-19 pandemic, the onslaught of ransomware attacks in 2020 has compounded civil society's ability to carry on business as usual. Corporations, governments, schools and everything in between have constantly been in the crosshairs of underground criminal groups, often left with very little recourse if they find their systems have been locked.

That lack of recourse doesn't mean there's an absence of effort to beat the bad guys. But even for seasoned professionals, it's a challenge to measure and quantify just how bad ransomware has gotten. While incidents continue to come to light, there is a lot the cybersecurity industry doesn't know: the volume of attacks, average cost of remediation and organizations who choose to stay silent once an attack has occurred.

What is known is that the criminal groups behind ransomware are flourishing, creating new variants and offering access on underground markets to anyone that has access to corporate networks and a desire to make a substantial amount of illicit money. Intel 471 has been tracking over 25 different ransomware-as-a-service crews over the past year, ranging from well-known groups that have become synonymous with ransomware, to newly-formed variants that have risen from the failures of old, to completely new variants that may have the ability to unseat the current top-level cabals.

The following is an examination of Ransomware-as-a-service (RaaS) crews that have grown over the past year. This is not meant to be a definitive measure of the ransomware scene, as what could be considered "damaging" — payment amount, system downtime, communications with attackers — could vary by crew or incident. Additionally, there are known private gangs operating in tight, close-knit criminal circles using direct and private communication channels that we have little visibility into.

What we are aiming to do is shine light on an area where relative darkness has led to a staggering amount of criminals running roughshod over enterprises, escaping with people's hard-earned money while facing very limited consequences. By speaking publicly on these operations, society as a whole can get a better understanding of the rising problem at hand.

TIER 3: Emerging RaaS Crews

We can verify that the following variants have been created and are being sold on a RaaS model, but at the present time, there is limited to no information on successful attacks, volume of attacks, payments received or cost of mitigation.

Name	Date Discovered	Notable Incidents	Markets Sold	Blog
CVartek.u45	March 2020	None	Torum	No
Exorcist	July 2020	None	XSS	No
Gothmog	July 2020	None	Exploit	No
Lolkek	July 2020	None	XSS	No
Muchlove	April 2020	None	XSS	No
Nemty	September 2020	None	XSS	Yes
Rush	July 2020	None	XSS	No
Wally	February 2020	None	Nulled	No
XINOF	July 2020	None	Private Telegram channel	No
Zeoticus	1.0 Dec. 2019, 2.0 Sept 2020	None	XSS/Private channels	No

TIER 2: Rising Powers

The following variants have been tied to a number of confirmed attacks, the frequency of which have grown over 2020. A number of these variants have utilized blogs to "name and shame" victims who have refused to pay ransoms.

Name	Date Discovered	Attack claims	Markets Sold	Blog
Avaddon	March 2020	Under 10	Exploit	Yes
Conti	August 2020	142	Private	Yes
Clop	March 2020	Over 10	N/A	Yes

DarkSide	August 2020	Under 5	Exploit	Yes
Pysa/Mespinoza	August 2020	Over 40	N/A	Yes
Ragnar	December 2019	Over 25	Exploit	Yes
Ranzy	October 2020	1	Exploit & XSS	Yes
SunCrypt	October 2019	Over 20	Mazafaka	Yes
Thanos	August 2020	Over 5	Raid	No

TIER 1: Most Wanted

These variants are among the most utilized, constantly showing up in enterprises that have been publicly linked to an attack. The variants are often iterations of past RaaS operations that were either shut down or broken up by law enforcement. All of these variants have utilized blogs to “name and shame” victims who have refused to pay ransoms. In all, these variants have pulled in hundreds of millions in ransoms -- a figure that may be low due to the lack of reporting surrounding enterprises payment to crews.

DoppelPaymer

DoppelPaymer, around since 2019, is associated with the BitPaymer aka FriedEx ransomware. CrowdStrike has highlighted some similarities between those variants, speculating that DoppelPaymer might be the work of the former BitPaymer group members.

The ransomware itself is usually deployed manually after a network is compromised and sensitive data is exfiltrated. The DoppelPaymer team operates a Tor-based “Dopple leaks” blog, which is used to publish information about compromised companies and their stolen data.

The crew is behind such notable attacks as those on Mexican energy giant Pemex and an IT contractor that works with the U.S. federal government.

The most known and discussed victim of DoppelPaymer ransomware is one against Düsseldorf University Clinic in September 2020. The actors actually wanted to target the Düsseldorf University and addressed it in the ransom note, but ended up hitting the hospital. When the perpetrators were made aware, they sent a digital key to get the hospital up and running again.

DoppelPaymer has been used in over 125 ransomware incidents in 2020.

Egregor/Maze

As this report was being published, the crew behind the Maze ransomware service announced it was shutting down its operations. There has been speculation that this group's affiliates will likely be funneled into the services behind Egregor ransomware. Egregor follows a familiar pattern in its operations: Compromise corporate networks to steal sensitive data and deploy ransomware, communicate with victims and demand ransoms, then dump sensitive data on a blog when victim organizations refuse to pay the ransom.

There is evidence that Egregor is also linked to Sekhmet ransomware. Intel 471 researchers found Egregor contained the same Base64 encoded data as Sekhmet where the last row contained additional parameters from a compromised system. Researchers also found that Egregor ransom notes were strikingly similar to ones used with Sekhmet.

Egregor was found in incidents at Crytek, Ubisoft and Barnes & Noble.

Intel 471 found that Maze was used in over 250 ransomware incidents in 2020. Egregor was used in more than 200 incidents.

Netwalker

First detected in September 2019, NetWalker is one of the more prolific affiliate services Intel 471 has tracked. The actors behind it have spent 2020 using phishing emails that leverage the impact and fear of the COVID-19 pandemic to lure victims into loading their malware onto systems. In May, the operators launched a Tor-based blog to release sensitive data stolen from victim organizations that refused to pay the requested ransom.

The actors used a fileless infection technique and allegedly could bypass the user account control component of Windows 7 and newer operating systems. NetWalker could be operated in two modes: In "network mode," individual computers or the entire network could be held for ransom and the victim could purchase a decryption tool with a master key or buy the necessary keys to decrypt certain computers. In "individual mode", a ransom was demanded for a single computer at a time.

The most high-profile target hit by Netwalker is Michigan State University, which refused to pay the ransom.

Netwalker has been tied to 143 ransomware incidents in 2020.

REvil

One of the most ubiquitous ransomware variants on the market, deployments of REvil first were observed on April 17, 2019, where attackers leveraged a vulnerability in Oracle WebLogic servers tracked as CVE-2019-2725. Two months later, advertisements started popping up on the XSS forum.

REvil has been one of the most active ransomware gangs in recent memory, claiming responsibility for such attacks as those on U.K.-based financial service provider Travelex, U.S.-based entertainment and media law firm Grubman Shire Meiselas & Sacks and 23 local governments in Texas.

One of the most common ways the group gains access to organizations is through remote desktop protocol (RDP) vulnerabilities, such as the BlueGate vulnerability, which allows remote code execution by an authorized user. The representative admittedly preferred to use information stealers to obtain remote access credentials, which are then used to secure an initial foothold in company networks. In the case of the Travelex and Grubman Shire Meiselas & Sacks attacks, the representative said networks were compromised by exploiting outdated Citrix and Pulse Secure remote access software, with the actors allegedly gaining access to an entire network in "about three minutes."

While the group carries out attacks on its own, it has found the RaaS model brings back more money. Affiliates are responsible for gaining access to target networks, downloading valuable files and deploying the actual ransomware, while the REvil gang handles victim negotiations and blackmailing, ransom collection and distribution. This model has apparently led to skyrocketing profits: according to the REvil representative, one affiliate's earnings rose from about US$20,000 to US $30,000 per target with another RaaS offering to about US $7 million to $8 million per target in only six months after joining forces with REvil.

Intel 471 has linked REvil to 230 ransomware attacks in 2020.

Ryuk

The name “Ryuk” could arguably be categorized as synonymous with ransomware, as the variant is one of the most popular, with a strong affiliate program and a large list of victims.

It is often delivered as the last action in the chain of infections brought on by dueling use of the Trickbot botnet and Emotet malwares. (Intel 471 has previously covered that relationship.) Recently, we have also witnessed that Ryuk is delivered through the Bazar loader.

Affiliates follow a model in their attacks: Hiring actors to launch spam campaigns to deliver the actor's banking malware. Then, another set of actors conduct privilege escalation attacks within compromised corporate networks. Then, teams of as many of five deploy the ransomware and handle negotiations with victims.

Ryuk has exploded over the past year, responsible for millions of ransomware incidents around the world. Some security researchers estimate that Ryuk has been found in as much as one-third of ransomware attacks launched this year.

One of the biggest threats from Ryuk this year has been focused on the healthcare sector. The attack that drew the most headlines was the attack on Universal Health Services, one of the biggest hospital systems in the United States.

While the cybersecurity community recognizes the threat all of these groups present, the criminals are only one part of the picture. In our next entry, Intel 471 will examine what a business goes through once it has to recover from a ransomware attack.