The Most Prolific Ransomware Families: A Defenders Guide

domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide

Executive Summary

Ransomware dominates the news cycle, but with an ever-growing number of variants and the botnets behind them it's easy for defenders to lose track of their relationships. In this article, DomainTools researchers provide a look at the three most prolific (by victim) ransomware families and the current loaders they use.

Ransom-every-ware

The current cybersecurity news cycle seems entirely dominated by the ransomware scene as major pipelines are interrupted, the meat supply chain grinds to a halt, and manufacturers across the board shutter while getting their networks in order. Ransomware gangs appear to be multiplying and new groups are claiming their ties to older groups to gain clout and scaring their victims into payment. Affiliate programs are recruiting on hacker forums while initial access brokers are selling footholds into corporate networks. There is a vast underground economy booming around the ransomware scene today.

In all of this, it's easy to get lost when examining infections as the deluge of incidents continues. Malware families like TrickBot, Ryuk, Dridex, BazarLoader, and DoppelPaymer certainly don't make things any easier for defenders. Ransomware gangs or affiliate groups being confounded with their tooling names muddle things even further. Couple that with the fact that most of these hacker tools have precursor tools that lead to infections, a partnership where a botnet operator, after acquiring what they need from a network, then sells access or directly works with ransomware groups for a cut of their take. These partnerships are akin to partnerships in the corporate world: for example, a TrickBot infection often leads to Conti or Ryuk ransomware or a Qakbot infection leads to a REvil ransomware. These ties and alliances shift as new botnets and groups bloom and fade.

Through this article, DomainTools research will give a lay of the land, as it stands today, and which infections lead to what outcomes, properties of those infections, and how to spot them. We'll concentrate on the top three most prolific ransomware families by number of victims Conti, Maze (and in turn Egregor, more on that later), and Sodinokibi (REvil) to provide you with a better comprehension of what you read in the ever-evolving ransomware news cycle.

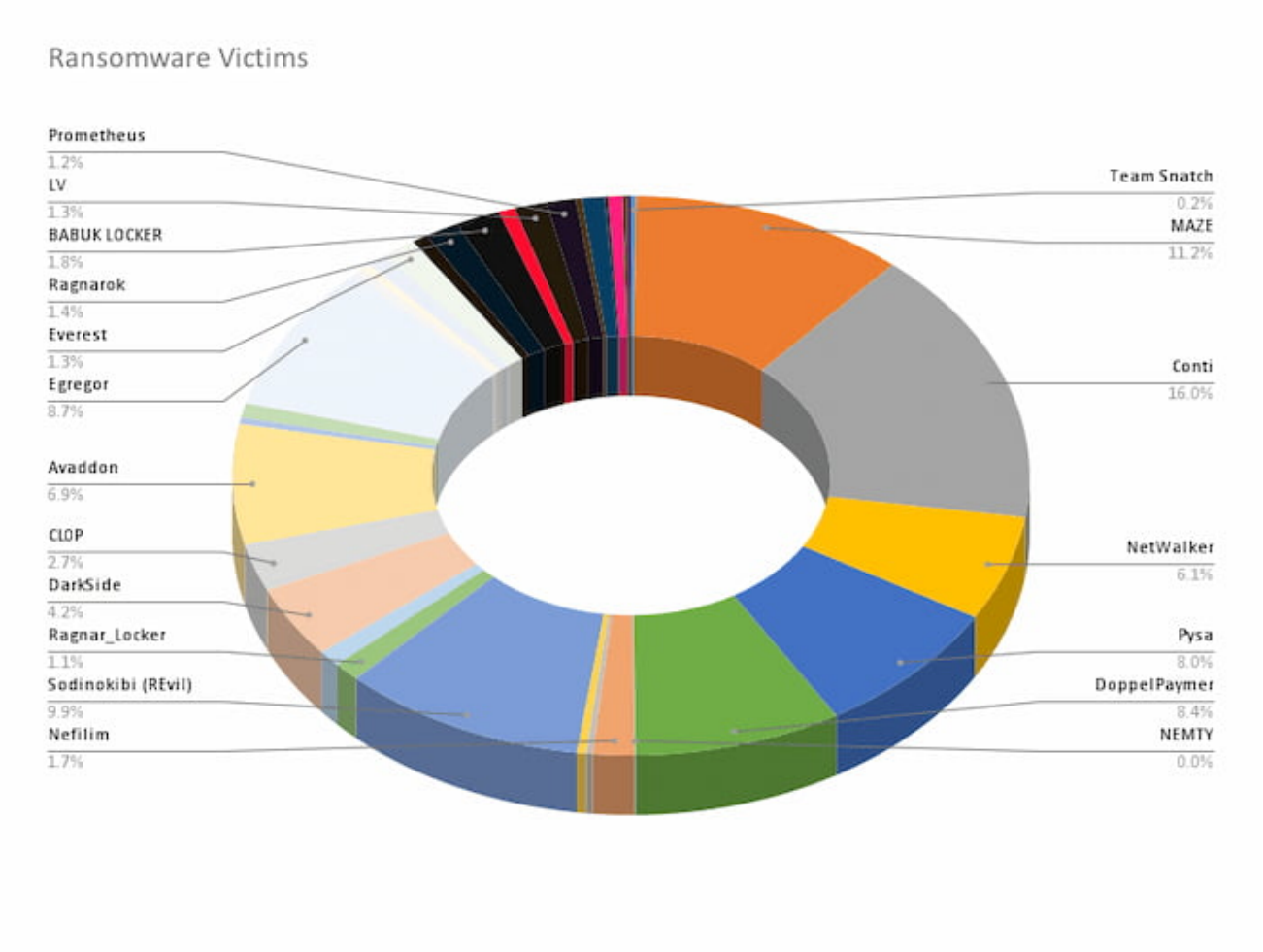


Image courtesy of Allan Liska

An Important Reminder On Affiliates

DomainTools researchers feel that it is important to remind readers that all of these groups make alliances, share tools, and sell access to one another. Nothing in this space is static and even though there is a single piece of software behind a set of intrusions there are likely several different operators using that same piece of ransomware that will tweak its operation to their designs.

The playbook of the affiliate programs that many of these ransomware authors run is to design a piece of ransomware and then sell it off for a percentage of the ransom gained. Think of it as a cybercrime multi-level marketing scheme. Often there is a builder tool that allows the affiliate to customize the ransomware to their needs for a specific target which at the same time tweaks the software slightly so it can evade standard, static detection mechanisms. This article's intent is not to dive deep into tracking individual affiliates or into each of the stages of a piece of packed malware (looking at you, CobaltStrike), but just to the top level of software used and their relations.

Lastly, we must mention that access for the ransomware is often being provided by an initial backdoor or botnet, frequently called an initial access broker. These backdoors, sometimes referred to as remote access trojans (RATs), are first dropped by a downloader, another piece of simple, obfuscated software that is usually distributed by spam emails with malicious documents of varying types. Sometimes, the people behind these RATs and ransomware families will also obtain access by password spraying techniques or exploiting old vulnerabilities that might be present on aging systems exposed on corporate networks. We will include those steps in our explanations.

> All in all, what this shows is that the problem space to look in for a robust defense solution isn't necessarily at the ransomware itself, but the methods of initial access through spam email campaigns, brute force attacks, and vulnerability management. Rarely are the affiliates behind the ransomware infection actually the same entity acquiring initial access.

Conti

First observed in December 2019, Conti is suspected to be operated by the same group that is behind the Ryuk ransomware, known for its rapid cycles of initial access to ransomware infection. Like many groups, they operate a Ransomware-as-a-Service (RaaS) offering and have a leak site that they leverage against victims for double extortion. While distributed by the TrickBot botnet in the past, Conti is often seen now being distributed by Bazar and IcedID (aka BokBot). What's interesting here is that IcedID was also known to be distributed by the prolific Emotet botnet which distributed TrickBot and Ryuk in the past as well. All of these connections lead most to believe that the groups behind all of these pieces of malicious software are connected and working together.

Conti is unique in that when encrypting victim data with AES256, the software uses a multithreaded approach which makes the execution much faster than other malware families. This can mean that by the time defenders notice the Conti infection on one machine, it's far too late to remediate. The ties to older groups such as Ryuk, having operated since 2018, and the improvement in capabilities and speed indicate that Conti is the next iteration of software for these gangs and the most deadly of the current malware families. Additionally, the fact that Conti is one of the few RaaS programs that sometimes gains initial access on its own shows a higher level of sophistication than some other affiliate groups.

Lastly, we want to call out Bazar for a piece of uniqueness uncovered by the domain name-specific research that DomainTools conducts. Bazar uses EmerDNS blockchain-based domains. This is an alternative domain registry which uses EmerCoin as the blockchain, meaning the domains cannot be taken down or sinkholed to disrupt the botnet's communications as this is an entirely separate DNS not under anyone's control. Use of these blockchain domains has been slowly on the rise in malicious softwares and produces a significant problem for defenders.

Maze and Egregor

The Maze ransomware group remains one of the most prolific ransomware affiliate programs with such a vast number of infections that they still exist in the top ten infections of all time even though the affiliate program announced their retirement in November 2020 after only forming in 2019. Maze, previously called ChaCha for its use of the ChaCha encryption algorithm, was also the first RaaS to develop a leaks site and attempt to get victims to pay using double extortion—something that's common for all new ransomware programs today. For that reason we couldn't leave them off this list even though most of their affiliates moved on to using the Egregor ransomware, first appearing in September 2020, after Maze's retirement.

Maze used off-the-shelf exploit kits such as Fallout or Spelevo and spam campaigns that have downloaders that install Cobalt Strike Beacon. Beacon is a commercial, full-featured RAT that is found in almost all infection chains these days. Despite claiming to be a tool for red teams and penetration testers, Cobalt Strike is so full-featured, particularly its modular command and control in Beacon, that bad actors have taken the tool up without abandon. Most infection chains have an instance of Beacon in them somewhere, including with Conti above.

What's important to note here is that the Egregor ransomware family departs from Maze in that it follows a similar model to Conti where external exploits against RDP, similar to Conti, are used as well as spam mail with malicious documents to drop the Qakbot (AKA Qbot) worm. Qakbot is a commodity malware, available since 2007, that is available on a number of underground forums and used by several ransomware families. Muddying waters even further, Qakbot has been seen being dropped by Emotet in some infections and tied to

several ransomware families in the past outside Egregor, such as ProLock and LockerGoga. The Egregor attacks using RDP to gain an initial foothold lead some to believe that some Egregor affiliates are confident in breaching networks directly while others are relying on initial access brokers who are less skilled leveraging commodity malware.

REvil (Sodinokibi)

The REvil ransomware family first appeared in April 2019 and is thought, due to code similarities, to be the spiritual successor to GandCrab, an earlier ransomware variant that targeted consumers. Similar to many other ransomware variants, REvil checks on startup if the computer's language region is set to an allowlisted country, typically a nation outside of the CIS nations such as Kazakhstan and Russia. Much like other families, REvil operates a leak site where they have for instance offered up stolen Apple blueprints.

REvil also has a number of unique features that make the malware particularly sinister. For instance, REvil samples will attempt to escalate privileges by constantly spamming the user with an administrator login prompt or will reboot into Windows Safe Mode to encrypt files, as antivirus software rarely runs in safe mode. The software also uses a custom packer to disguise itself which makes analysis difficult for less talented reverse engineers. Separate from the previous two families discussed, REvil uses the AES or Salsa20 encryption algorithms on victim files which is a slightly unique signature. These unique features along with the RaaS' success has led to some new gangs, such as Prometheus, claiming to be a part of REvil to encourage victim payment.

As for distribution, REvil affiliates have been seen using a spam campaign to deliver malicious documents and exploit kits targeting old vulnerabilities on unpatched machines as well as most recently through Qakbot. This new relationship of being distributed through the Qakbot worm brings REvil into line with the many other families that have been distributed by botnets in the past. With the speed at which many of these ransomware groups are now moving and the money involved, purchasing access from botnet operators into valuable victim networks is more effective than individual targeting of companies for most affiliates.

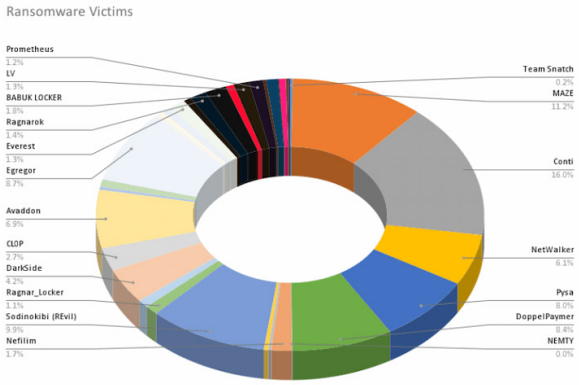
Ransomware Map

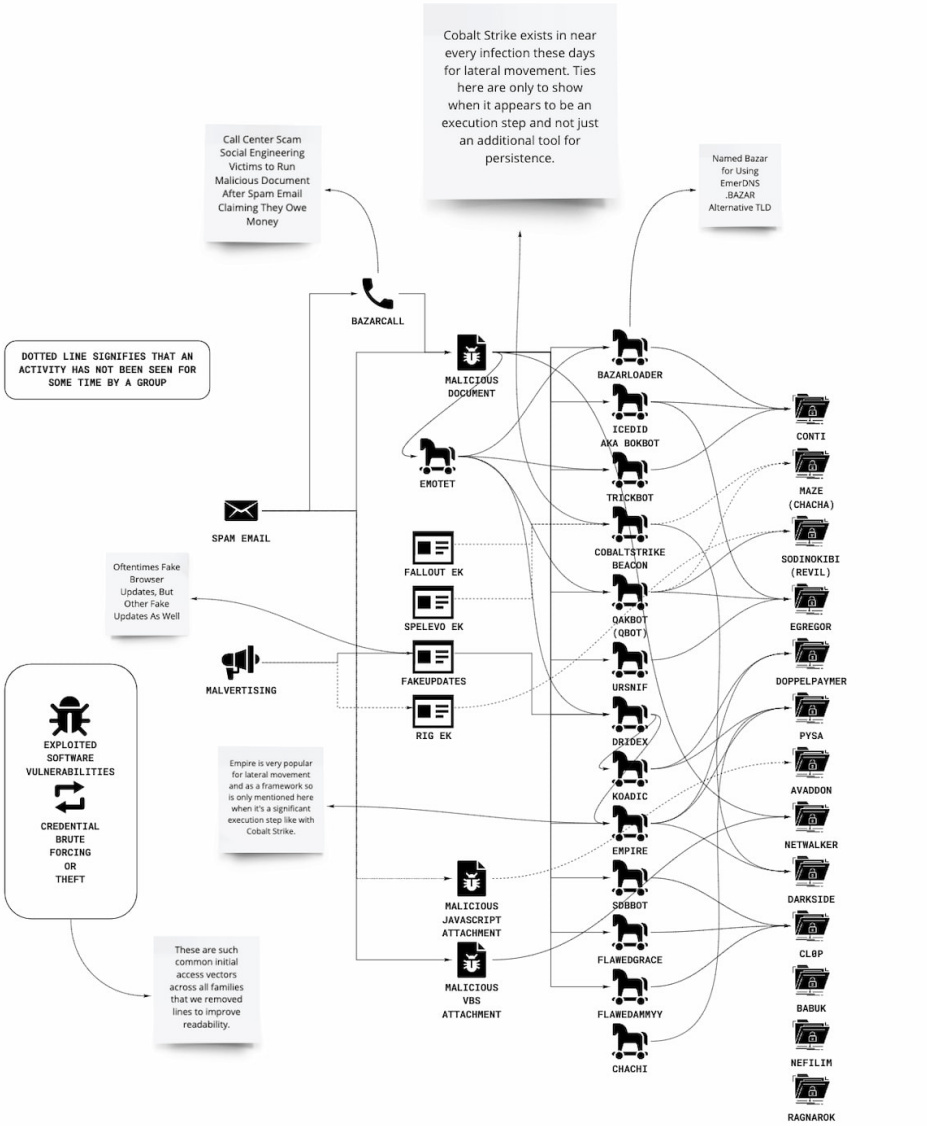
While the previous three families may be the most prominent in terms of victim market share, there remains an ever growing number of ransomware gangs and families to keep track of in the rapid news cycle. These three families also offer a glimpse into what most of the ransomware market looks like as far as infection vectors and chains are concerned. With those as a basis, we offer the was a guide below to help with interpreting any articles encountered on ransomware. As with any ancient map there are portions of unknown territories (here be dragons) and portions that may rapidly shift from the time when this map was made. Tactics and techniques change, relationships change, but this is the market slightly untangled from the DomainTools research perspective at the time of this publishing.

RANSOMWARE INFECTIONGRAPHIC
UPDATED JUNE 2021

This graphic is the result of reading dozens of ransomware reports over the last several years and an attempt to make some sense out of the complex, interwoven relationships between ransomware families and the initial access stages. It is by no means complete as tactics shift constantly, but the aim is to provide a reference point when reading about infections.

Ransomware victim marketshare graph courtesy of Allan Liska.





CONTI
ACTIVE: MAY 2020 - PRESENT
EXTENSIONS: RANDOM
ENCRYPTION: AES
NOTES: CONTI_README.TXT
UNIQUE NOTES:
- MULTITHREADED ENCRYPTION
- AKA/SUCCESSOR TO RYUK

MAZE
ACTIVE: MAY 2019 - NOV 2020
EXTENSIONS: PER-FILE RANDOM
ENCRYPTION: CHACHA/RSA
NOTE: DECRYPT-FILES.TXT
UNIQUE NOTES:
- AKA CHACHA RANSOMWARE
- CALLED OUT SEVERAL SECURITY RESEARCHERS IN JANUARY 2020 BY NAME
- MANY SKILLED EVASION AND ANTIDEBUGGING TECHNIQUES

REVIL
ACTIVE: APR 2019 - PRESENT
EXTENSIONS: PER-VICTIM RANDOM
ENCRYPTION: SALSA20/AES
NOTE: {RANDOM-EXT}-HOW-TO-DECRYPT.TXT
UNIQUE NOTES:
- CONSIDERED SUCCESSOR TO GANDCRAB
- BOOTS INTO SAFE MODE TO AVOID EDR

EGREGOR
ACTIVE: SEP 2020 - PRESENT
EXTENSIONS: PER-HOST RANDOM
ENCRYPTION: SALSA20
NOTE: RECOVER-FILES.TXT
UNIQUE NOTES:
- PART OF SEKHMET RANSOMWARE FAMILY
- CONSIDERED SUCCESSOR TO MAZE

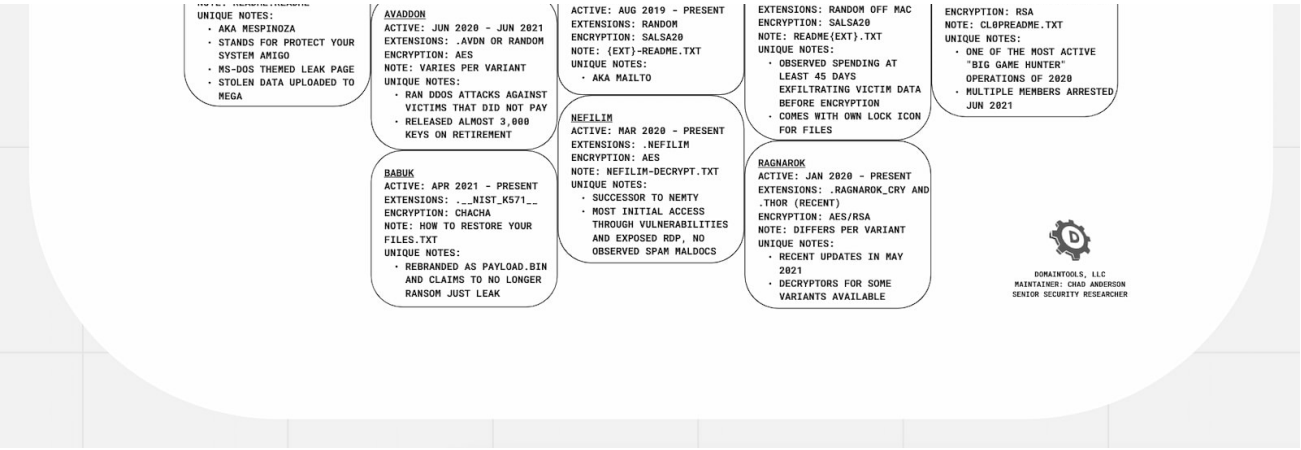
DOPPELPAYMER
ACTIVE: APR 2019 - PRESENT
EXTENSIONS: .LOCKED
ENCRYPTION: RSA/AES/RC4
NOTE: {FILENAME}.README
2UNLOCK.TXT
UNIQUE NOTES:
- CONSIDERED SUCCESSOR TO BITPAYMER (AUG 2017)

PYSA
ACTIVE: OCT 2019 - PRESENT
EXTENSIONS: .PYSA
ENCRYPTION: AES
NOTE: README.README

NETWALKER

DARKSIDE
ACTIVE: AUG 2020 - PRESENT

CL0P
ACTIVE: FEB 2019 - PRESENT
EXTENSIONS: .CL0P/.CLOP/.CLLP



Click here to view the full Miro board.