2020: The year in malware

blog.talosintelligence.com/2020/12/2020-year-in-malware.html

By Jon Munshaw.

Nothing was normal in 2020. Our ideas of working from offices, in-person meetings, hands-on learning and basically everything else was thrown into disarray early in the year. Since

then, we defenders have had to adapt. But so have workers around the globe, and those IT and security professionals in charge of keeping those workers' information secure.

Adversaries saw all these changes as an opportunity to capitalize on strained health care systems, schools scrambling to adapt to online learning and companies who now had employees bringing home sensitive information and data while working on their personal networks. This led to a huge spike in ransomware attacks and headlines all over of companies spending millions of dollars to recover their data and get back to work quickly.

Oh, and there was a presidential election this year, too, which came with its own set of challenges.

To recap this crazy year, we've compiled a list of the major malware, security news and more that Talos covered this year. Look through the timeline below and click through some of our other blog posts to get caught up on the year that was in malware.

- **January**

  Attackers used several popular and well-known file-hosting services to avoid blocklisting and deliver a threat we called "JhoneRAT," mainly to Arabic-speaking targets.

- **February**

  Another RAT, "ObliqueRAT," used malicious Microsoft Office documents to infect diplomatic and government agencies/organizations in Southeast Asia. Cisco Talos also discovered a link between ObliqueRAT and another campaign from December 2019 distributing CrimsonRAT.

- **March**
  - As the COVID-19 pandemic hit the United States, workers across the country and globe had to begin working from home full-time. As the pandemic was the biggest news story of the year, hitting its peak in mid-March, attackers started using news around COVID-19 to spread malware.
  - The pandemic also presented a platform for adversaries to spread disinformation around the virus and associated government relief packages.

April

- Cisco Talos researchers highlighted some of the problems with using fingerprint scans to protect your devices. We cloned fingerprints using a few different methods and tested their ability to unlock certain devices, showing that you shouldn't use biometric scanners as the last line of defense for vital data or devices.
- Python-based PoetRAT used COVID-19-themed lures to target government agencies and everyday users in Azerbaijan, also capitalizing on the country's ongoing military and civil conflicts.
- Online meeting software exploded in popularity, which created a fresh target for attackers looking to spread malware or just generally be disrupted. One such example was this vulnerability in the Zoom meeting software Talos discovered, though there are many more exploits out there for all sorts of meeting software.
- The Aggah malspam campaign expanded its reach, now delivering Agent Tesla, njRAT and Nanocore RAT.

May

- Thai Android devices and users are targeted by a modified version of DenDroid we called "WolfRAT," now targeting messaging apps like WhatsApp, Facebook Messenger and Line.
- Brazilian users are targeted with the Astaroth malware family, which used YouTube as a unique command and control (C2) to help evade detection.

June

- IndigoDrop utilizes military-themed malicious maldocs to spread Cobalt Strike beacons containing full-fledged RAT capabilities. These maldocs use malicious macros to deliver a multistage and highly modular infection.
- The PROMETHIUM actor expands its reach and tries to infect new targets in Colombia, India, Canada and Vietnam by teaming up with StrongPity3.

July

- The wave of ransomware attacks hits a peak. Specifically, WastedLocker targeted some big-name companies and organizations looking to make headlines and rake in big paydays.
- We released our first research paper in a series covering election security and disinformation ahead of the November presidential election.
- The Prometei botnet adds multiple ways to spread, deploying a Monero-focused cryptocurrency miner.

- **September**
  - A new campaign we dubbed “Salfram” spreads various malware payloads including Gozi ISFB, ZLoader, SmokeLoader and AveMaria, among others.
  - With many students returning to school totally online, we spotted a spike in online homework scams, with sites promising to write papers and complete assignments for a fee, though many of them turned out to be phony or even deliver malware.
  - LodaRAT shows it’s adding new features and obfuscation techniques.

- **October**
  - The Lemon Duck cryptocurrency-mining botnet uses several new techniques likely to be spotted by defenders but would largely go undetected by end users while the adversary stole their computing power.
  - The DoNot APT group experiments with new methods of delivery for their payloads. They used a legitimate service within Google's infrastructure which makes it harder for detection across a user's network.
  - The FBI and U.S. Cybersecurity and Infrastructure Security Agency released an alert warning health care systems to look out for a wave of ransomware attacks, corresponding in a rise in COVID-19 cases.

- **November**
  - A new version of the CRAT malware pops up in the wild with sandbox evasion techniques and a new modular plugin framework.
  - Emotet completes its 2020 comeback with a huge November and October, increasing its activity across the globe after it largely went quiet over the summer.

- **December**

  We uncover the Xanthe cryptocurrency miner after it tried to compromise one of Cisco's security honeypots for tracking Docker-related threats.