# Malware Trends: What’s Old Is Still New

It’s clear that cybercrime is one of the world’s most lucrative illicit industries – possibly taking the top spot. Threat actors are getting more meticulous and inventive in their ploys, even reviving outdated and long-forgotten techniques, thanks to their own brand of Key Performance Indicators linked to return on investment. After all, if a successful remake of an old classic can generate new revenue, producers will embrace it.

Many of the most successful cybercriminals are shrewd; they want good ROI, but they don’t want to have to reinvent the wheel to get it. That’s one reason they are leveraging existing infrastructure and older threats to maximize opportunity. As a security professional, you need to know what attackers are up to so you can focus your resources appropriately.

**Remaking the classics**

When the FortiGuard Labs research team looked at the second half of 2022, code reuse (old code being retrofitted into new versions) and the re-emergence of well-known names in the botnet, malware and wiper space – such as Emotet and GandCrab, among others – served as a reminder that threats and malware never truly go away. They merely retreat underground and wait for another opportunity. And they are available wholesale any time to anyone who wants to buy them.

In fact, the majority of the top malware observed was more than a year old. Some malware types were antiquated by cybersecurity standards. Many lawful software initiatives

recycle code to create fresh applications on an established foundation, which allows room for improvement. Each version also has the potential to branch out and develop into something distinct, and the code can be improved upon, modified and released again.

What does it then look like when criminals alter their "applications" in this way? Let's look at Emotet as an example.

**Emotet just won't quit**

Emotet, first discovered as a banking trojan in 2014, continues to wreak havoc. The malware familied, which steals sensitive and private information from victims' computers, has infected more than a million devices and is considered one of the most dangerous threats of the decade. More recently, it's been spread through malicious Microsoft Office files, called maldocs, which are included in phishing emails. An Excel 4.0 Macro or a VBA Macro is used to run malicious code that downloads and starts the Emotet malware as soon as the victim opens the associated document.

Researchers investigated the propensity of 98 different Emotet variations to "borrow" code amongst themselves. We discovered that Emotet had undergone significant speciation in the nine years since it originally surfaced. We discovered that these 98 variants can be divided into about six different "species" of malware using fairly sophisticated network community detection algorithms, practically all of which share at least some of their code.

What started as a banking Trojan has been adapted to become a malware distribution botnet. Emotet spreads using spam messages, and after it has accessed a system, it keeps doing so by connecting to the contacts list of that system. Emotet disappeared in January 2021, but it is resilient and came back in November of that year with a vengeance. Conti, the criminal

organization based in Russia, is thought to have used Emotet up to May 2022, when the group was shut down.

Emotet is robust because it mainly depends on polymorphism for its packer, allowing it to easily get around legacy AV tools. The creators of Emotet are also changing how they behave, adjusting tactics to avoid detection and increasing the likelihood that their intended targets will open their spam emails. After seizing control of a computer, it exploits the victim's email account and inbox to launch subsequent attacks.

**Combatting the retro trend**

Winning the war against code reuse and variant frequency is about response time. Your ability to defend against, identify, and neutralize such risks quickly determines the success of your security stance and your ability to keep your enemies out. Clouds, networks, endpoints and email must all have automated and centrally managed defenses. Using strategies like segmentation throughout the distributed network makes it simpler to detect and stop lateral movement across your infrastructure when architectural designs change.

Last but not least, analytics powered by machine learning will assist in correlating atypical behaviors into a warning that requires immediate assessment and action. AI/ML-based tools can also detect new mutations of virus like Emotet. For businesses determined to protect their environment, operationalizing the MITRE ATT&CK system on attackers' TTP profiles and regularly testing fresh tactics against your cybersecurity tools are essential. Solutions and services for attack simulation can aid in gap analysis and closure.

**Defeating dangerous trends**

Like cable reruns of our favorite childhood TV shows, everything old is new again in the world of malware. But unlike those shows, malware is not a welcome diversion but a serious threat that must be proactively addressed. Emotet is

just one example of the current malware reboot trend that organizations need to be aware of. Use the defensive strategies noted above to defend against this dangerous retread.

https://www.securityweek.com/malware-trends-whats-old-is-still-new/