

2019 Threats Predictions McAfee Labs

Partners in Cybercrime

Cybercriminals will band together, creating fewer but stronger malware-as-a-service families.



One-Stop Attack Shops

Cybercriminals can buy malware, exploits, botnets, and other shady services on the underground market. Criminals of varying experience and sophistication can easily launch attacks.



Underground Consolidation

Malware-as-a-service families will actively work together. These alliances will flourish via affiliates—such as exploit kits boosting ransomware (GandCrab).





Strong Brands Expand Reach

Increasingly powerful brands will propel more sophisticated cryptocurrency mining and increases in mobile malware and stolen credit cards and credentials.



Exploitation

Cybercriminals will become more agile. In 2019 they will exploit short-lived vulnerabilities, reducing the time from detection to weaponization.

and avoiding detection.

Evasion Techniques

The prevalence of attack outsourcing will lead to use of artificial intelligence in evasion tactics.



cybercriminals will become more agile and better able to circumvent protections. coin miner stopping when Task Manager runs or during a scan, exploit kits using process injection or manipulating memory space to insert code, botnets adding obfuscated code to slow reverse engineering,

and APTs using stolen certificates to avoid detection.

Which Attack Is It?

Synergistic attacks involving multiple threats working together act as a smokescreen, hindering defenders from identifying an actor's ultimate goal.



Data Exfiltration Attacks to Target the Cloud

More Data to Steal

As enterprises continue to fully adopt multiple cloud models (SaaS, PaaS, IaaS), more data resides in the cloud than ever before. Attacks will follow the data and increasingly target these cloud services.





MITM Attacks

GhostWriter: Leveraged the cloud as a springboard for cloudnative man-in-the-middle attacks **to launch cryptojacking or ransomware attacks.**



Office 365 a Target

KnockKnock: With the increased adoption of Office 365, there has been a surge of attacks—especially attempts to compromise email, such as **the botnet KnockKnock**, which targeted system accounts without multifactor authentication.

Voice-Controlled Digital Assistants

New Entry to the Home

As voice-controlled digital assistants are increasingly used to manage all the IoT devices within a home, they will be a preferred entry point into a home network for cybercriminals.



Identity Platforms and Edge Devices Under Siege

Large-scale identity platforms offer centralized secure authentication and authorization of users, devices, and services across IT environments—and a focus for criminals.





Social Media

Despite increased security efforts by platform providers, their data-rich environments will continue to be a lucrative target for cybercriminals. This will be the next big battleground.

Edge Devices

Adversaries will continue to launch remote attacks against edge devices any network-enabled system hardware or protocol within an IoT product—due to static password use and limited security.



Broken Trust

The IoT trust model is built on a weak foundation of assumed trust and perimeter-based security. Most IoT edge devices provide no self-defense by default so one successful exploit owns the device.



Securing Our Systems

Multifactor authentication and identity intelligence will become the best methods to provide security in this escalating battle.

Rise of Misinformation Against Corporations

Fake news and extortion campaigns via social media will attack brands, originating not from nation-state actors but from criminal groups.



Misleading Content

Botnet accounts disseminate and promote messages, often on BOTH sides of a story to spur debate. Messages that perform best are further amplified to extort companies by threatening their brands.

Rapid Spread

One bot account with 279 followers, mostly other bots, began harassing an organization. With amplification, the account gained 1,500 more followers in only four weeks by simply tweeting malicious content about their target.

Read the full *McAfee Labs Threats Predictions Report* Visit: <u>www.mcafee.com/2019Predictions</u> for the full report.

