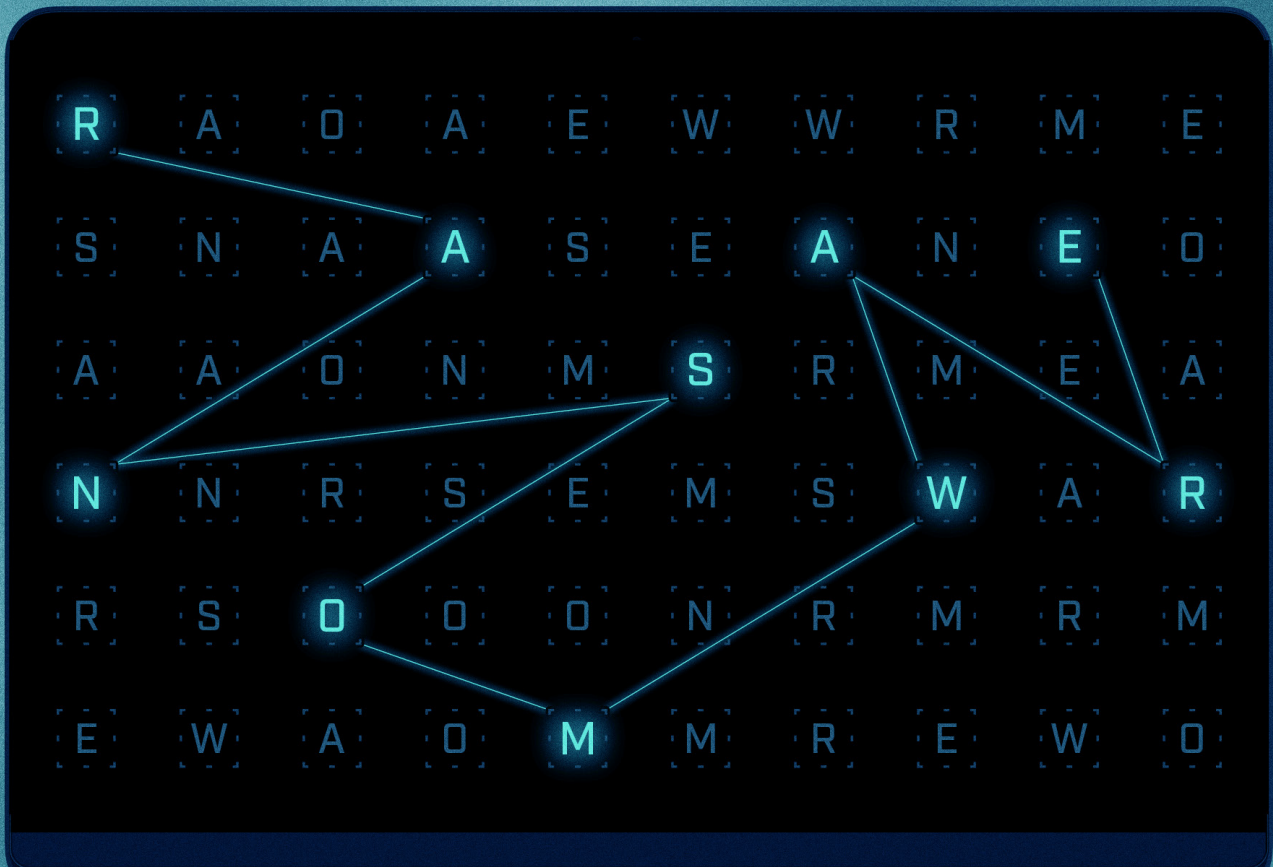


RANSOMWARE DECODED

Understanding and Preventing Modern Ransomware Attacks



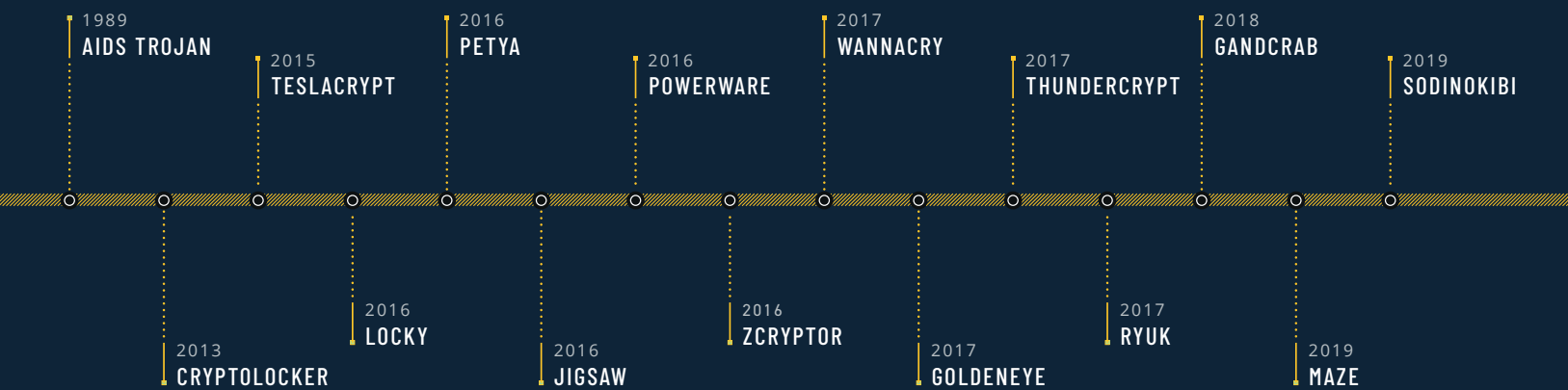
Ransomware is Here to Stay

Though ransomware attacks dropped significantly in early 2018, over the past several years they have reemerged with a vengeance. Ransom payments have also shot up; in December 2019 the average ransom payout to an attacker was over \$80,000. Today's attackers are not only holding data ransom, but stealing it to sell on the Internet. This shows a trend where attackers aren't just executing ransomware, they are persisting on the network, successfully exfiltrating data, and then finally deploying ransomware.

Ransomware is Evolving

Many types of malware silently persist on the network, move laterally, communicate with their C2, or obfuscate their behaviors to prevent detection. In contrast to this, traditional ransomware was all about coming in with a big splash and causing immediate damage. The goal was to get on the machine and ransom data, and that was it. The sooner the malware could encrypt files, the less risky the attack, and the more likely the attacker would make money.

THE EVOLUTION OF RANSOMWARE



This focused, singular objective resulted in a lot of simple, quick, and sometimes ugly malware. Much of Cybereason's early research into ransomware shows just that: while some were very sophisticated, others were quite crude. However, this does not stop the ransomware from being effective; in fact, quickly developing crude ransomware and spamming unsuspecting users continues to be a very cost-effective attack vector.

Because ransomware operates so differently than other types of malware, it can be challenging to detect. Combined with obfuscation techniques and vulnerabilities that allow remote code execution, ransomware is able to evade legacy prevention solutions to achieve its goal.

Modern ransomware is taking a slightly different approach. Instead of limiting themselves to leveraging ransomware to exclusively collect a ransom, attackers are now deploying malware that steals credentials and persists in the network for an extended period of time before deploying ransomware. This method has the potential for much greater bang for the buck, as attackers can sell off stolen credentials, move to infect other machines on the network, and ultimately deploy the actual ransomware.

Anyone Can Initiate a Ransomware Attack

With the advent of **Ransomware-as-a-Service (RaaS)**, even non-technical users can leverage ransomware to attack organizations globally. The Cybereason team has observed many malware authors **leveraging the Malware-as-a-Service model** to make money consistently. Like many modern MaaS, RaaS gives non-technical and technical users alike easy access to damaging and exploitative software through the proverbial swipe of a credit card. This continues the ongoing adoption of modern MaaS to create a new group of cybercriminals that profit off of other, less technical cybercriminals.

Many of their methodologies also overlap with that of legitimate software-as-a-service (SaaS) businesses: underground marketing efforts, relying on positive reviews, responsive customer support, and regularly improving features in their product, which are all hallmarks of a profitable SaaS.

Maintaining Backups or Paying the Ransom Won't Always Work

More often than not, the prevailing advice when preparing for a ransomware attack is to **maintain secure backups of all your data**. This is reasonable advice, however, backups should be part of a broader, layered defense strategy -- not the first or only line of defense. Many security teams today are taking the post-breach mindset, as a focused attacker can almost always breach prevention defenses. Much like defending royal jewels in a castle, the jewels may be secured in a safe, but you still have a moat, gate, guards, and locks to prevent attackers from even reaching the safe. Naturally, attackers **also look to target backups themselves**, potentially rendering them useless.

Further, even in cases where organizations paid the ransom, **17% of them** were unable to recover their data anyway. Those that can recover their data are always at risk that the decryption tool they are provided is unstable or ineffective.

Even if you do pay and are able to recover all your data, there will still be significant man hours lost from an attack. MSPs reported that solely the cost of downtime from an attack was **23 times greater than the ransom** the attacker requested, resulting in damage to the brand and potentially business-damaging disruption. It typically results in over **16 days of downtime** for an organization. Over two weeks of business disruption can dramatically change the success of a business.

Bottom line, ransomware attacks are dangerous even if you maintain backups, and potentially costly even if you pay the ransom quickly.

What Modern Ransomware Looks Like

RYUK RANSOMWARE (FEAT. EMOTET & TRICKBOT)

The Cybereason Nocturnus team researched a campaign that used a multi-stage attack to stealthily **deliver the Ryuk ransomware**. This spanned from Emotet's delivery of TrickBot, to TrickBot's information stealing capabilities, lateral movement, and use as a downloader for Ryuk, and finally to Ryuk's ransomware capabilities. With Ryuk, the attacker is able to encrypt the machine and ransom data back to the victim, with the potential to cost victims significant sums of money due to downtime, recovery costs, and damage to reputation.

TAKEAWAY: Many companies impacted by Ryuk weren't just hit by ransomware, but also additional malware that collects credentials and persists on the network. This is further confirmation that ransomware attacks are evolving to damage organizations as much as possible.

GANDCRAB

The Cybereason Nocturnus team dissected [a campaign to deliver the GandCrab ransomware](#) to an international company based in Japan. GandCrab was one of the most prevalent ransomwares in the threat landscape and was constantly evolving and perfecting its delivery methods to evade detection.

Bitdefender estimates that GandCrab is responsible for 40% of all ransomware infections globally, which demonstrates exactly how effective it has become. The authors are known to iteratively and quickly update GandCrab with stealthy new delivery mechanisms and other adaptations.

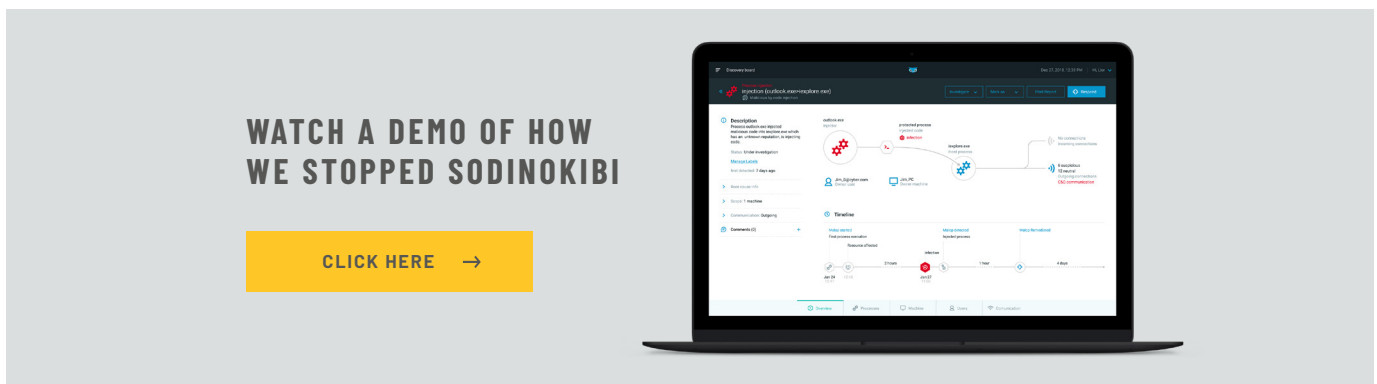
TAKEAWAY: Before being retired, GandCrab had many variants and continues to evolve. The only way to reliably prevent this ransomware is through security tools that can identify and correlate behaviors, and not just signatures. If you'd like to test if this can be detected in your environment, we'd be happy to walk you through the process.

SODINOKIBI

The Cybereason Nocturnus [team analyzed Sodinokibi](#), a highly evasive ransomware that takes many measures to prevent its detection by antivirus and other means. The authors of Sodinokibi have previously been connected to the same authors of the prolific GandCrab ransomware, which was recently retired.

When Sodinokibi first emerged, it exploited vulnerabilities in servers and other critical assets. As time went by, it also leveraged other infection vectors such as phishing and exploit kits. There were several instances where the Sodinokibi ransomware purposefully searched for an AV made by South Korean security vendor Ahnlab in an attempt to inject its malicious payload into the trusted AV vendor.

TAKEAWAY: Sodinokibi is another ransomware that uses a suite of tricks, including obfuscated PowerShell commands, to evade existing defenses. This highlights the need to have comprehensive prevention and detection on the endpoint.



SECURITY RECOMMENDATIONS TO PREVENT RANSOMWARE ATTACKS

1. Keep secure backups following the [3-2-1 rule](#). Keep 3 copies of your data, store 2 copies on different storage media, and ensure 1 copy is kept off-site.
2. Train your organization on how to [identify and remove phishing emails](#), a common method used by attackers to gain an initial hold on the network.
3. Invest in a [leading endpoint protection platform](#) that incorporates multiple layers of endpoint prevention, including

ABOUT CYBEREASON

Cybereason gives the advantage back to the defender through a completely new approach to cybersecurity: the Cybereason Defense Platform. Cybereason offers managed, as-a-service, and on-premise prevention, detection and response solutions. Cybereason technology delivers multi-layer endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Cybereason is privately held and is headquartered in Boston, Massachusetts, with offices around the globe.

Visit our website to learn more

CLICK HERE →

FOLLOW US

