# ShurL0ckr Ransomware as a Service Peddled on Dark Web, can Reportedly Bypass Cloud Applications

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shurl0ckr-ransomware-as-a-service-peddled-on-dark-web-can-reportedly-bypass-cloud-applications

Security researchers uncovered a new ransomware named ShurL0ckr (detected by Trend Micro as RANSOM_GOSHIFR.B) that reportedly bypasses detection mechanisms of cloud platforms. Like Cerber and Satan, ShurL0ckr's operators further monetize the ransomware by peddling it as a turnkey service to fellow cybercriminals, allowing them to earn additional income through a commission from each victim who pays the ransom.

The researchers' analysis of ShurL0ckr indicates it can evade detection by cloud applications where it's reported to proliferate. Like other ransomware, phishing and drive-by downloads are their likeliest infection vectors.

ShurL0ckr's discovery was part of a larger problem: cybercriminals abusing legitimate platforms and services. The researchers noted that 44% of businesses using cloud applications were in some way affected by malware. In fact, they found at least three enterprise software-as-a-service (SaaS) applications infected with malware. The researchers also found malicious scripts and executables, as well as Trojanized Office documents and image files, to be the most commonly used entry point.

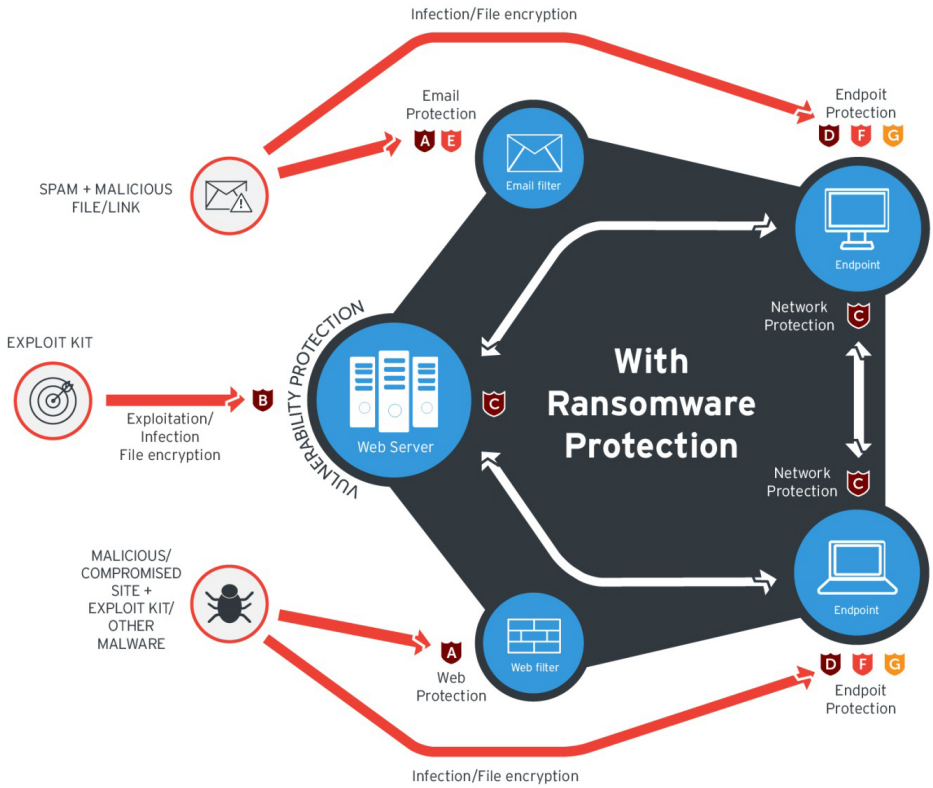
**[RELATED NEWS: Security Flaw in Google Apps Script can Let Hackers Deliver Malware via SaaS Platform]**

Indeed, ransomware isn't going away any time soon. In fact, it's projected to be a cybercriminal mainstay, along with digital extortion, as organizations increasingly incorporate emerging technologies to conduct business.

How exactly does RaaS figure into this? It lowers barriers to entry. Typically, a developer will write the malware, build its infrastructure, then make it accessible to others regardless of their technical knowhow. This business model continued to boom into 2017, as evidenced by

the 2,502% growth in ransomware's economy in the dark web. A lifetime license to WannaCry ransomware, for instance, was sold for just $50 in the Middle Eastern and North African underground two days after its outbreak in May last year.

Indeed, RaaS thrived in 2017—with the likes of Satan promising easy buck and FrozrLock guaranteeing "unlimited builds" to Karmen, Nemes1s RaaS, PadCrypt, and Fatboy, touting premium customer service. ShurL0ckr exemplifies how outsourcing malware puts threats into more cybercriminal hands, resulting in ever-increasing builds of similar malware in the wild with varying degrees of capabilities, and constantly fine-tuned to evade traditional security mechanisms.




*A multilayered defense against ransomware*

Given ShurL0ckr's nature, the ransomware can be customized — from the ransom demand and encryption capabilities to how it's delivered, which makes defense in depth significant. Here are some best practices users and organizations can adopt to mitigate threats like ShurL0ckr:

- Regularly back up files and ensure their integrity and accessibility
- Keep the system, its applications, and the network updated; employ virtual patching for end-of-life and legacy systems
- Secure or restrict the use of tools typically reserved for system administrators to prevent their abuse
- Incorporate multilayered security mechanisms such as data categorization, network segmentation, application control/whitelisting, and behavior monitoring
- Enable the firewall, sandbox, and deploy intrusion detection and prevention systems

- Nurture cybersecurity awareness: Beware of social engineered email and develop proactive incident response and remediation strategies to mitigate further exposure

## Trend Micro Solutions

Enterprises can benefit from a multi-layered, step-by-step approach in order to best mitigate the risks brought by these threats. Email and web gateway solutions such as Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevent ransomware from ever reaching end users.

At the endpoint level, Trend Micro Smart Protection Suites deliver several capabilities like high-fidelity machine learning, behavior monitoring and application control, and vulnerability shielding that minimize the impact of this threat. Trend Micro Deep Discovery Inspector detects and blocks ransomware on networks, while Trend Micro Deep Security™ stops ransomware from reaching enterprise servers–whether physical, virtual or in the cloud.

Trend Micro's Cloud App Security (CAS) can help enhance the security of Office 365 apps and other cloud services such as Google Drive by using cutting-edge sandbox malware analysis for ransomware and other advanced threats.

These solutions are powered by Trend Micro XGen™ security, which provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. Smart, optimized, and connected, XGen™ powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

HIDE

**Like it? Add this infographic to your site:**
1. Click on the box below.  2. Press Ctrl+A to select all.  3. Press Ctrl+C to copy.  4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Ransomware