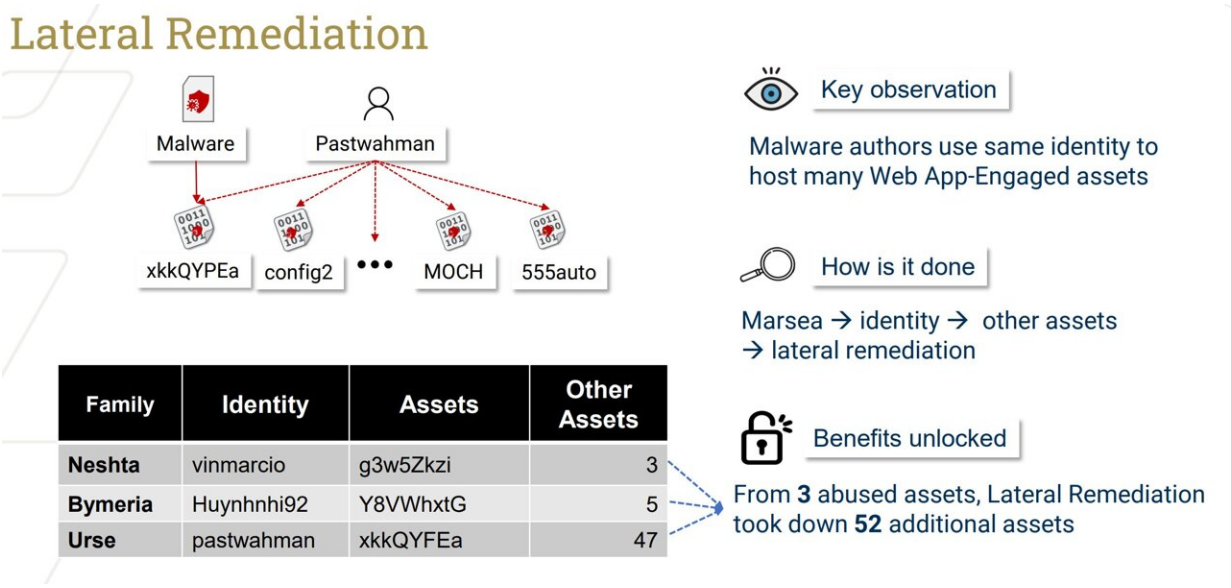
Playing hide and seek with a new breed of malware threatening millions of users

September 11 2023, by John Popham



Credit: Georgia Institute of Technology

Lurking just under the surface of popular online applications like Dropbox and Discord is a threat lying in wait to infect users unlucky enough to cross its path.

Findings produced by Georgia Tech's Cyber Forensics Innovation (CyFI) Lab reveal this new type of menace, labeled as web app engaged (WAE) malware by the lab, has seen an increase of 226% since 2020. Fortunately, the team created a tool that enables cybersecurity incident

responders to purge nearly 80% of discovered WAE malware by collaborating with service providers.

"Web applications have become an integral part of our online lives, offering various services such as content delivery, data storage, and social networking," said Mingxuan Yao, Georgia Tech Ph.D. student. "Unfortunately, these utilities have made web applications an attractive playground for malware creators. WAE malware is designed to exploit these applications, posing several risks to users."

WAE malware operates deceptively, though not in the ways one might expect. Rather than compromising the security of the web applications, this type of malware abuses the applications by making its malicious traffic appear benign. By doing so, it effectively hides in plain sight, enabling it to carry out its activities without being detected.

Addressing these threats requires a coordinated effort between incident responders and web app providers. Still, such collaboration has been lacking until now. The research produced by CyFI Lab seeks to enable such cooperation and provide insights into the prevalence and the characteristics of WAE malware.

Yao and his co-authors created Marsea to comprehensively examine WAE malware automatically. The tool identifies and separates abuse based on a web app's identity and assets.

When used on a group of 10,000 malware samples, Marsea found nearly a thousand instances of malware throughout 29 different web applications. Alarmingly, Marsea also revealed that attackers are transitioning their malicious command-and-control servers to these web apps to evade detection. The research team has used Marsea to collaborate with web app providers to take down 79.8% of the malicious web app content.

In August, the team presented "Hiding in Plain Sight: An Empirical Study of Web Application Abuse in Malware" at the 32nd USENIX Security Symposium.

More information: Hiding in Plain Sight: An Empirical Study of Web Application Abuse in Malware; www.usenix.org/conference/usen … ntation/yao-mingxuan

Provided by Georgia Institute of Technology