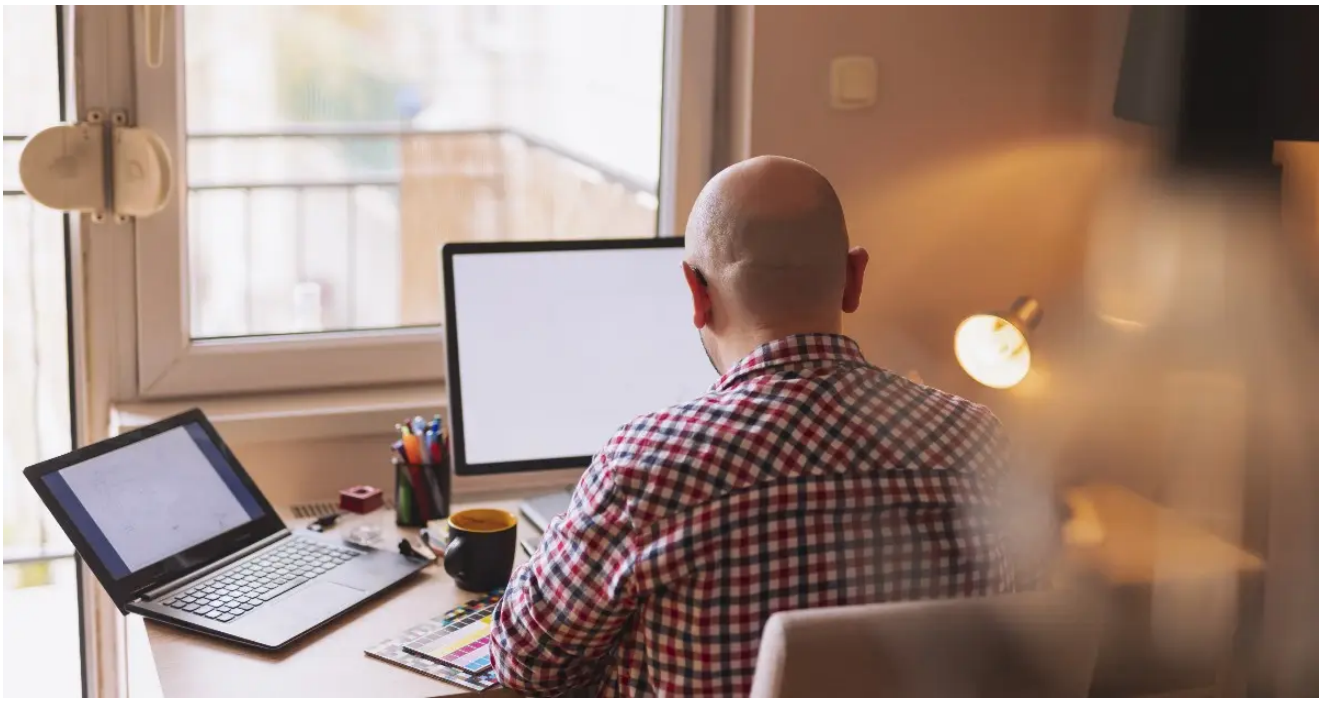
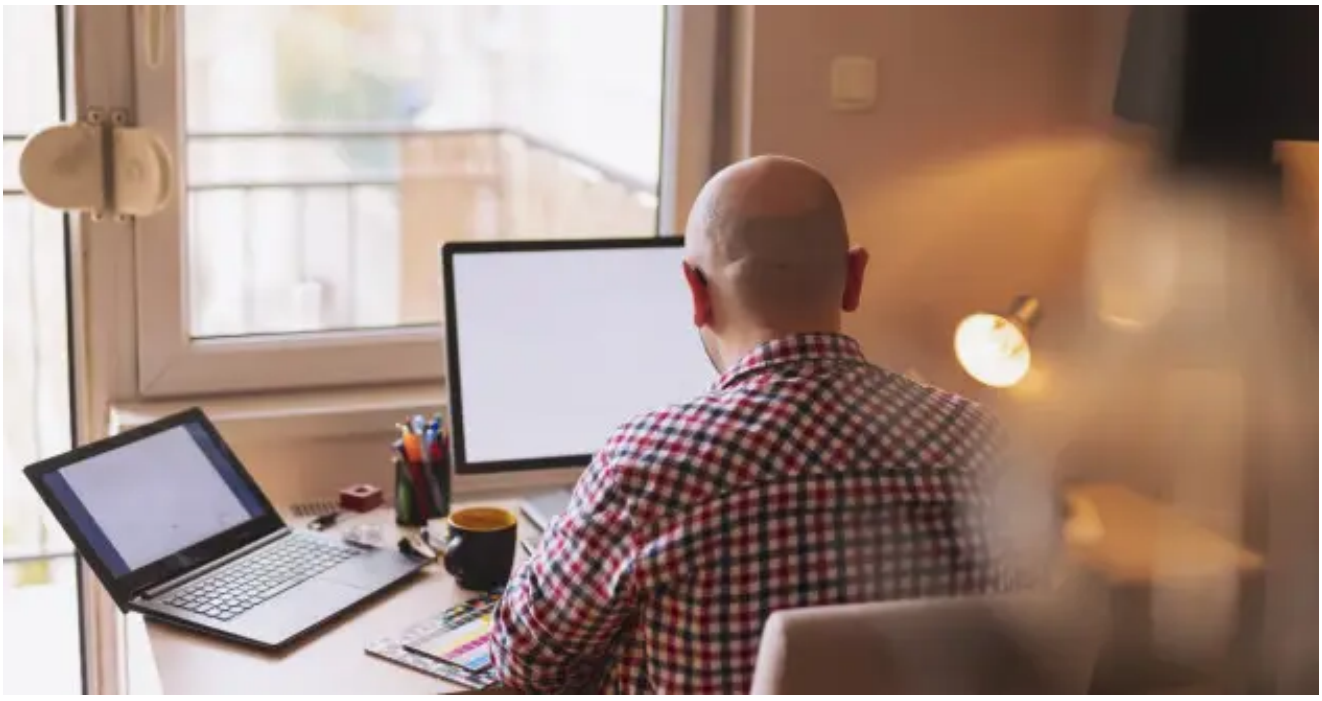
Top-Ranking Ramnit Banking Trojan Looking to Steal Payment Card Data

securityintelligence.com/posts/ramnit-banking-trojan-stealing-card-data/



Home / Advanced Threats

Top-Ranking Banking Trojan Ramnit Out to Steal Payment Card Data



Advanced Threats January 31, 2022

By Limor Kessem co-authored by Itzik Chimino 4 min read
Shopping online is an increasingly popular endeavor, and it has accelerated since the COVID-19 pandemic. Online sales during the 2021 holiday season rose nearly 9% to a record $204.5 billion. Mastercard says that shopping jumped 8.5% this year compared to 2020 and 61.4% compared to pre-pandemic levels.

Cyber criminals are not missing this trend. The Ramnit Trojan, in particular, is out for a shopping spree that's designed to take over people's online accounts and steal their payment card data.

IBM X-Force researchers follow malware activity and targeting year-round. They have seen a diverse collection of Ramnit configuration files over the years. Not only was Ramnit the top active banking Trojan for 2021, but this malware has also been a cyber crime tool for well over a decade. It continues to target people and service providers when it is the online shopping season.

Most recently, the Ramnit malware infected a long list of brands and online retailers, clearly switching into holiday shopping mode. Among the top brands are travel and lodging platforms, with Ramnit targeting people looking to get away for the holidays.

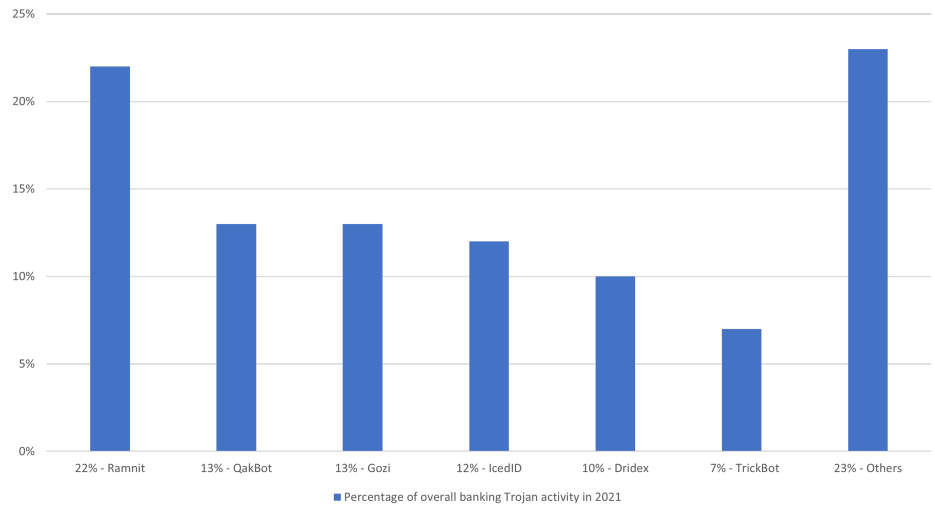


Figure 1: Top active banking Trojans in 2021

Ramnit: Taking Over Accounts Since 2010

Ramnit carries out simple yet effective operations on infected devices. While other cyber crime gangs have moved on to larger corporate bounties and ransomware/extortion attacks, Ramnit continues to focus on consumers. Once it is resident on an infected device, it monitors browsing to target websites and goes into information stealing mode. It typically snatches login credentials, but its web injections can also trick victims into providing payment card details or other personal data.

In the current web injection IBM X-Force analyzed, Ramnit uses an external script that's pulled into web sessions in real-time from its remote server. The look and feel of the injection are identical, and all injections come from the same command and control servers:

hxxps://lillllilillilllillil[.]com/cc/js/

hxxps://lillllilillilllillil[.]com/ba/js/

The pop-up victims see on screen when they access a compromised URL asks them to type in their payment card details. Typically, this information is used for card-not-present fraud, whether online or over the phone.

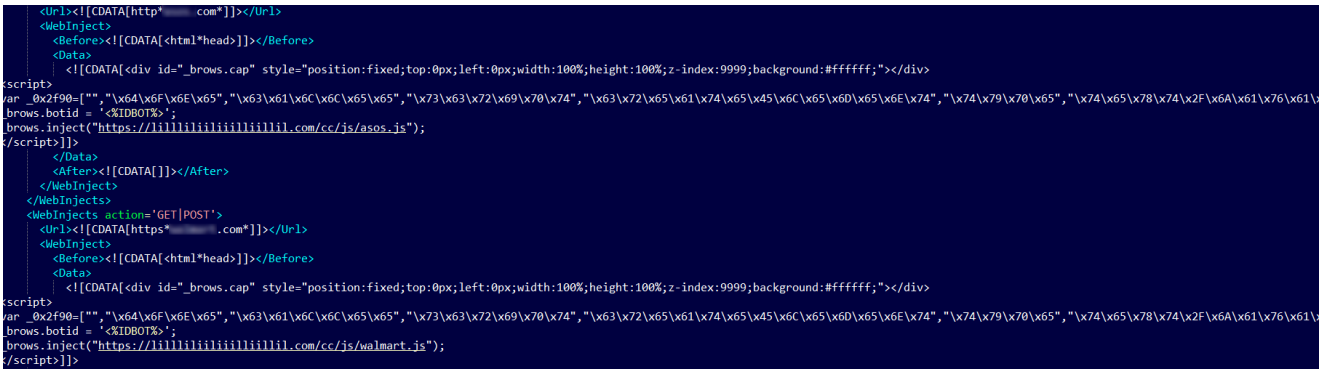


Figure 2: Simplistic injections are used for all targets, asking for payment card data

This injection utilizes string literals replacement and encodes them in Hex or Unicode as part of the obfuscation process. For example:

var _0x2f90 = [“”, “\x64\x6F\x6E\x65”, “\x63\x61\x6C\x6C\x65\x65”, “\x73\x63\x72\x69\x70\x74”, “\x63\x72\x65\x61\x74\x65\x45\x6C\x65\x6D\x65\x6E\x74”, “\x74\x79\x70\x65”, “\x74\x65\x78\x74\x2F\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74”, “\x73\x72\x63”, “\x3F\x74\x69\x6D\x65\x3D”, “\x61\x70\x70\x65\x6E\x64\x43\x68\x69\x6C\x64”, “\x68\x65\x61\x64”, “\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x73\x42\x79\x54\x61\x67\x4E\x61\x6D\x65”, “\x76\x65\x72”, “\x46\x46”, “\x61\x64\x64\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\x65\x6E\x65\x72”, “\x44\x4F\x4D\x43\x6F\x6E\x74\x65\x6E\x74\x4C\x6F\x61\x64\x65\x64”, “\x72\x65\x61\x64\x79\x53\x74\x61\x74\x65”, “\x63\x6F\x6D\x70\x6C\x65\x74\x65”, “\x6D\x73\x69\x65\x20\x36”, “\x69\x6E\x64\x65\x78\x4F\x66”, “\x74\x6F\x4C\x6F\x77\x65\x72\x43\x61\x73\x65”, “\x75\x73\x65\x72\x41\x67\x65\x6E\x74”, “\x49\x45\x36”, “\x6D\x73\x69\x65\x20\x37”, “\x49\x45\x37”, “\x6D\x73\x69\x65\x20\x38”, “\x49\x45\x38”, “\x6D\x73\x69\x65\x20\x39”, “\x49\x45\x39”, “\x6D\x73\x69\x65\x20\x31\x30”, “\x49\x45\x31\x30”, “\x66\x69\x72\x65\x66\x6F\x78”, “\x4F\x54\x48\x45\x52”, “\x5F\x62\x72\x6F\x77\x73\x2E\x63\x61\x70”, “\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64”, “\x64\x69\x73\x70\x6C\x61\x79”, “\x73\x74\x79\x6C\x65”, “\x6E\x6F\x6E\x65”,

“\x68\x74\x6D\x6C”, “\x70\x6F\x73\x69\x74\x69\x6F\x6E”, “\x66\x69\x78\x65\x64”, “\x74\x6F\x70”, “\x30\x70\x78”, “\x6C\x65\x66\x74”, “\x77\x69\x64\x74\x68”, “\x31\x30\x30\x25”, “\x68\x65\x69\x67\x68\x74”, “\x7A\x49\x6E\x64\x65\x78”, “\x39\x39\x39\x39\x39\x39”, “\x62\x61\x63\x6B\x67\x72\x6F\x75\x6E\x64”, “\x23\x46\x46\x46\x46\x46\x46”];

When de-obfuscated, this turns out to be:

var _0x2f90 = [“”, “done”, “callee”, “script”, “createElement”, “type”, “text/javascript”, “src”, “?time=”, “appendChild”, “head”, “getElementsByTagName”, “ver”, “FF”, “addEventListener”, “DOMContentLoaded”, “readyState”, “complete”, “msie 6”, “indexOf”, “toLowerCase”, “userAgent”, “IE6”, “msie 7”, “IE7”, “msie 8”, “IE8”, “msie 9”, “IE9”, “msie 10”, “IE10”, “firefox”, “OTHER”, “_brows.cap”, “getElementById”, “display”, “style”, “none”, “html”, “position”, “fixed”, “top”, “0px”, “left”, “width”, “100%”, “height”, “zIndex”, “999999”, “background”, “#FFFFFF”];

With these generic injections, researchers are seeing Ramnit target a plethora of e-commerce brands and accounts with leading retailers. Some hospitality giants are also on Ramnit’s target list.

A Top Banking Trojan for Over a Decade

Ramnit is a top-ranking banking malware that has been active in the wild since 2010. Ramnit started out as a self-replicating worm, leveraging removable drives and network shares to spread to new endpoints. As the project evolved, Ramnit morphed into a banking Trojan.

In 2011, Ramnit’s developer apparently decided to borrow chunks of code from the leaked Zeus Trojan v2 source, which effectively turned Ramnit into a banking Trojan that steals user credentials and deploys in session web injections.

Between 2011 and 2014, the Ramnit Trojan gained momentum in the cyber crime arena, ranking in the top 10 list of the most prevalent financial malware codes. Ramnit infections were rampant in North America, Europe and Australia, where its local targets included a multitude of recruitment sites, likely for the purpose of recruiting mules.

Ramnit configurations were typically very long and characterized by a rather exhaustive list of online anti-malware scans, antivirus products’ websites, cyber crime information sites and security blogs. This list was designed to keep victims away from security controls that would identify the infection. In some cases, the mere use of the word “cyber crime” or “police” in the URL typed by victims triggered a redirection effect to a different website.

In late February 2015, a Europol operation, in collaboration with information security vendor Symantec, attempted to dismantle the Ramnit project by taking down botnets operated by the Ramnit gang. A few days later, another vendor (Dr. Web) released a blog post indicating

that the Ramnit botnet was still alive. By December 2015, IBM X-Force reported renewed Ramnit activity that targeted banks and e-commerce in Canada, Australia, the United States and Finland.

In the most recent campaigns, Ramnit is delivered in booby-trapped productivity files, most often through malicious macros.

According to IBM X-Force threat intelligence, Ramnit's source code remains the property of the gang that operates it and continues to be active as we move into 2022.

To keep up to date about malware campaigns and tactics, techniques and procedures, follow IBM X-Force research at: securityintelligence.com/category/x-force/

If your organization requires help in securing customers against banking Trojans, please visit the IBM Trusteer page: www.ibm.com/security/fraud-protection/trusteer

IOCs

C2 Servers

hxxps://lilllilililiiilliillil[.]com/cc/js/

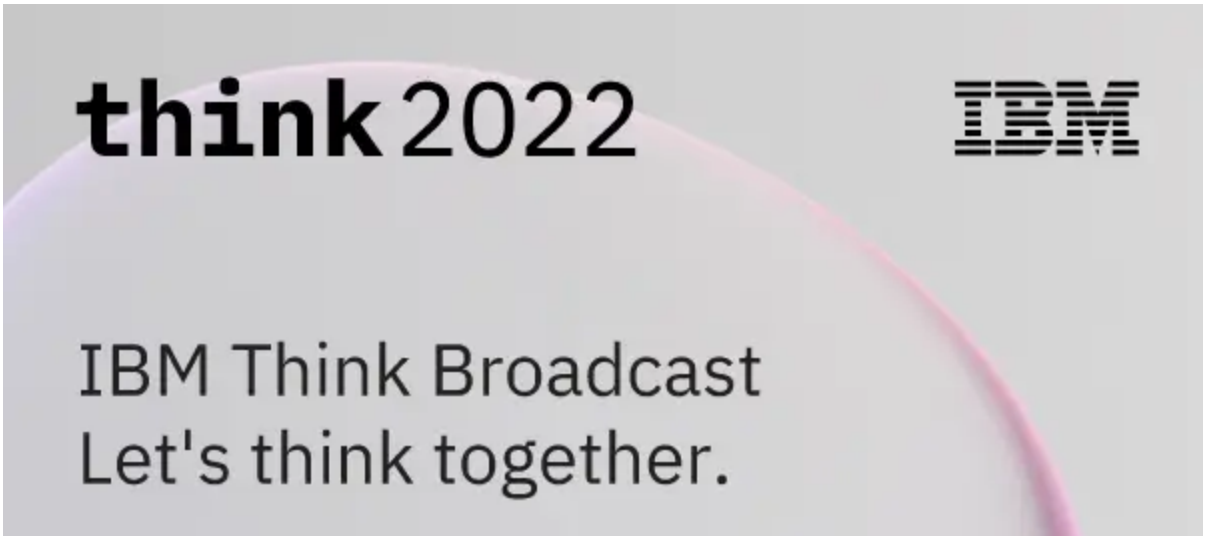
hxxps://lilllilililiiilliillil[.]com/ba/js/

Sample

MD5 Ramnit: d194da95c851f252e496229a90353bc9

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...




Watch on demand