LATAM financial cybercrime: Competitors-in-crime sharing TTPs

welivesecurity.com/2020/10/01/latam-financial-cybercrime-competitors-crime-sharing-ttps/

October 1, 2020

ESET researchers discover surprisingly many indicators of close cooperation among Latin American banking trojans' authors

ESET Research
1 Oct 2020 - 11:30AM

ESET researchers discover surprisingly many indicators of close cooperation among Latin American banking trojans' authors

ESET has published a white paper detailing its findings about interconnectivity of Latin American banking trojan families. The white paper was also published by Virus Bulletin.

For a long time, Latin American banking trojans were looked upon as one group of malware. ESET researchers discovered that is not the case and that, despite having so much in common, multiple distinct malware families can be recognized among these banking trojans. Over the past year, we have been publishing an ongoing blogpost series about Latin American banking trojan malware families. These blogposts focus mainly on the most important and interesting aspects of these families. So far, we have unmasked Amavaldo, Casbaneiro, Mispadu, Guildma, Grandoreiro and Mekotio in this series. In the pieces to come, we will continue with Krachulka, Lokorrito, Numando, Vadokrist and Zumanek.

LATAM financial cybercrime: Competitors-in-crime sharing TTPs

Download Research Paper

In this white paper, we look at these families from a higher-level perspective – rather than examining details of each family and highlighting their unique characteristics, we focus on what they have in common. If you've been following our series, you may have noticed some similarities between multiple families in our series, such as using the same uncommon algorithm to encrypt strings or suspiciously similar DGAs to obtain C&C server addresses.

The first similarities we spotted are in the actual implementation of these banking trojans. The most obvious one is the practically identical implementation of the banking trojans' cores – sending notification to operator, periodically scanning active windows based on name or title, and attacking via fake pop-up windows designed carefully in an attempt to lure out sensitive information from victims. Besides that, these malware families share uncommon third-party libraries, string encryption algorithms, and string and binary obfuscation techniques.

However, the similarities do not end there. When analyzing the distribution chains of these malware families, we realized they share the same core logic, too – they usually check for a *marker* (an object, such as a file or registry key value used to indicate that the machine has already been compromised), and download data in ZIP archives. Besides that, we have observed identical distribution chains ending up distributing multiple Latin American banking trojans. It is also worth mentioning that since 2019, the vast majority of these malware families started to utilize Windows Installer (MSI files) as the first stage of the distribution chain.

Latin American banking trojans share execution methods as well. They tend to bring their own tools bundled in the aforementioned ZIP archives. The two most common methods are DLL side-loading and abusing a legitimate AutoIt interpreter. Additionally, when using the former method, multiple families abuse the same vulnerable applications for that purpose (so-called Bring Your Own Vulnerable Software).

The term "Latin American banking trojan" comes from the region these banking trojans typically target – Latin America. However, since late 2019, we see several of them adding Spain and Portugal to the list of countries they target. Moreover, different families use similar spam email templates in their latest campaigns, almost as if this were a coordinated move as well.

Given so many similarities, one would expect the fake pop-up windows these banking trojans use to be shared too. In fact, the opposite seems to be the case. Even though the windows look similar (since they are designed to fool customers of the same financial institutions), we have not spotted multiple families using *identical* windows.

Since we do not believe it to be possible that independent malware authors would come up with so many common ideas and we also don't believe one group to be responsible for maintaining all these malware families, we conclude that these are multiple threat actors closely cooperating with each other. You can find detailed information about the similarities we briefly introduced here, in the whitepaper.

MITRE ATT&CK techniques

In the table below, which is an aggregate of the techniques based on the standard MITRE ATT&CK table, we illustrate many of the features Latin American banking trojans share. It is not an exhaustive list, but rather one that focuses on the similarities. It shows mainly that:

- phishing is the most common attack vector
- they heavily rely on scripting languages, mainly VBScript
- Registry Run key or Startup folder are the most common methods of persistence
- they all obfuscate either payloads or configuration data in some way
- they heavily favor DLL side-loading
- to steal credentials, they tend to use either fake pop-up windows or keyloggers
- they devote considerable effort to collect screenshots and scan for security software
- custom encryption algorithms are favored over established ones
- they do not exfiltrate all harvested data to the C&C server, but use different locations as well

Note: This table was built using version 7 of the MITRE ATT&CK framework. It was updated on May 5th, 2021, to include findings from our research into Ousaban.

Tactic	ID	Name	Amavaldo	Casbaneiro	Grandoreiro	Guildma	Krachulka	Lokorrito
Initial Access	T1566.001	Phishing: Spearphishing Attachment	✔	✔	✔	✔	✔	✔
T1566.002	Phishing: Spearphishing Link	✔	✔	✔	✔	✔	✔	✔
Execution	T1059.005	Command and Scripting Interpreter: Visual Basic	✔	✔	✔	✘	✔	✔
T1059.007	Command and Scripting Interpreter: JavaScript/JScript	✔	✔	✘	✔	✘	✘	✔
T1059.003	Command and Scripting Interpreter: Windows Command Shell	✘	✔	✔	✘	✔	✘	✔
T1059.001	Command and Scripting Interpreter: PowerShell	✔	✔	✘	✘	✘	✘	✔

Tactic	ID	Name	Amavaldo	Casbaneiro	Grandoreiro	Guildma	Krachulka	Lokorrito
	T1047	Windows Management Instrumentation	✔	✘	✘	✔	✘	✘	✔
	T1059	Command and Scripting Interpreter (In the context of Latin American banking trojans, this means the AutoIt scripting interpreter)	✘	✔	✘	✘	✔	✘	✔
Persistence	T1547.001	Boot or Logon Autostart execution: Registry Run Keys / Startup Folder	✔	✔	✔	✔	✔	✔
	T1053.005	Scheduled Task/Job: Scheduled Task	✔	✔	✘	✘	✘	✘	✘
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	✔	✔	✔	✔	✔	✔
	T1574.002	Hijack Execution Flow: DLL Side-Loading	✔	✔	✘	✔	✔	✔	✔
	T1497.001	Virtualization/Sandbox Evasion: System Checks	✔	✔	✔	✔	✔	✔	✔
	T1218.007	Signed Binary Proxy Execution: Msiexec	✔	✔	✘	✘	✘	✘	✔
	T1036.005	Masquerading: Match Legitimate Name or Location	✘	✔	✔	✔	✘	✘	✘
	T1197	BITS Jobs	✘	✔	✘	✔	✔	✘	✔
	T1112	Modify Registry	✔	✔	✔	✔	✘	✘	✘
	T1218.011	Signed Binary Proxy Execution: Rundll32	✘	✔	✘	✔	✘	✘	✘
	T1027.001	Obfuscated Files or Information: Binary Padding	✘	✔	✔	✘	✘	✘	✔
	T1220	XSL Script Processing	✔	✘	✘	✔	✘	✘	✔
Credential Access	T1056.002	Input Capture: GUI Input Capture (In the context of Latin American banking trojans, this means using custom, carefully crafted fake pop-up windows)	✔	✔	✔	✔	✔	✔
	T1056.001	Input Capture: Keylogging	✔	✔	✔	✘	✔	✔	✔
	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	✔	✔	✔	✔	✘	✔	✔
	T1552.001	Unsecured Credentials: Credentials In Files	✘	✔	✔	✔	✘	✘	✘
Discovery	T1010	Application Window Discovery	✔	✔	✔	✔	✔	✔
	T1518.001	Software Discovery: Security Software Discovery	✔	✔	✔	✔	✔	✔	✔

Tactic	ID	Name	Amavaldo	Casbaneiro	Grandoreiro	Guildma	Krachulka	Lokorrito
	T1082	System Information Discovery	✔	✔	✔	✔	✔	✔	✔
	T1083	File and Directory Discovery	✔	✔	✔	✔	✔	✔	✔
	T1057	Process Discovery	✘	✔	✔	✘	✔	✔	✔
Collection	T1113	Screen Capture	✔	✔	✔	✔	✔	✔	✔
	T1115	Clipboard Data	✔	✔	✘	✘	✘	✘	✔
Command and Control	T1132.002	Data Encoding: Non-Standard Encoding	✔	✔	✔	✔	✔	✔	✔
	T1571	Non-Standard Port	✔	✔	✔	✘	✔	✘	✔
	T1132.001	Data Encoding: Standard Encoding	✘	✔	✔	✔	✔	✘	✘
	T1568.002	Dynamic Resolution: Domain Generation Algorithms	✘	✘	✔	✘	✔	✘	✔
	T1568.003	Dynamic Resolution: DNS Calculation	✘	✔	✘	✘	✘	✘	✔
Exfiltration	T1048	Exfiltration Over Alternative Protocol	✔	✔	✔	✔	✔	✔	✔
	T1041	Exfiltration Over C2 Channel	✔	✔	✔	✔	✔	✔	✔

As you can see, Latin American banking trojans, while having their differences, have many crucial features in common.

1 Oct 2020 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion