Lazarus Targets Latin American Financial Companies

By By: Lenart Bermejo, Joelson Soares Nov 20, 2018 Read time: 4 min (951 words)

Published: 2018-11-20 · Archived: 2026-04-05 16:48:35 UTC

The cybercriminal group Lazarus, and particularly its subgroup Bluenoroff, has a history of attacking financial organizationsopen on a new tab in Asia and Latin America. There seems to be a resurgence of activity from the group, and recent events show how their tools and techniques have evolved. Just last week they were found stealing millionsopen on a new tab from ATMs across Asia and Africa. We also recently discovered that they successfully planted their backdoor (detected by Trend Micro as BKDR_BINLODR.ZNFJ-Aopen on a new tab) into several machines of financial institutions across Latin America.

We determined that these backdoors were installed on the targets' machines on September 19 2018, based mainly on the service creation time of the loader component. We also saw that the attack technique bears some resemblance to a previous 2017 Lazarus attack, analyzed by BAE Systemsopen on a new tab, against targets in Asia. The use of FileTokenBroker.dll was a key part of the group's attack in 2017, and they seem to have used the same modularized backdoor in the recent incident as well.

Our analysis of the backdoors used in the September 2018 attacks show that AuditCred.dll/ROptimizer.dll was similarly used:

	FileTokenBroker.dll (2017 attack)	**AuditCred.dll/Roptimizer.dll (2018 attack)**
Launch Method	Service	Service
Function	Loader Component	Loader Component
Working directory	%Windows%\System32	%Windows%\System32
Loaded Component Path	%Windows%\System32\en-US	%Program Files%\Common Files\System\ado
Loaded Component Blending	Blends with .mui files	Blend with ActiveX data Object dll files

Table1: Similarities of the Loader components in both incidents

Analysis of backdoors used in 2018

The Lazarus group used a series of backdoors in their 2018 attacks, employing a complicated technique that involves three major components:

- **AuditCred.dll/ROptimizer.dll** (detected by Trend Micro as BKDR_BINLODR.ZNFJ-A) – loader DLL that is launched as a service
- **Msadoz<*n*>.dll** (detected by Trend Micro as BKDR64_BINLODR.ZNFJ-A) – encrypted backdoor; **n = number of characters in the loader dll's filename**
- **Auditcred.dll.mui/rOptimizer.dll.mui** (detected by Trend Micro as TROJ_BINLODRCONF.ZNFJ-A) – encrypted configuration file

Figure 1: Loading sequence of the modularized backdoor

The loader DLL is installed as a service and uses different names (AuditCred and ROptimizer) on different machines. However, they still have the same capabilities and are essentially the same file. Its purpose is to load Msadoz<n>.dll in order to decrypt and execute it in memory.

Figure 2: AuditCred/ROptimizer Service

If successfully installed, this particular backdoor poses quite a threat to its target. It is capable of the following functions:

- **Collect file/folder/drive information**
- **Download files and additional malware**
- **Launch/terminate/enumerate process**
- **Update configuration data**
- **Delete files**
- **Inject code from files to other running process**
- **Utilize proxy**
- **Open reverse shell**
- **Run in passive mode — instead of actively connecting to the command and control (C&C) server, the backdoor will open and listen to a port then receive commands through it**

Once the backdoor is loaded, it will then load the encrypted configuration file Auditcred.dll.mui/rOptimizer.dll.mui to extract the C&C information and connect to it. The connection is necessary for conducting activities; and based on the backdoor's functions, these actions could be quite damaging to targets.

Figure 3: The first step of decryption will perform XOR on one byte using the previous adjacent byte, starting from the last byte and excluding the first byte

Figure 4: The second step uses RC4, using the first 0x20 bytes from the result of the first step as the RC4 key

Figure 5: Encrypted (Top) and decrypted (bottom) configuration file

It is also important to note that while the loader component and the configuration file are located in the same directory (%windows%\system32), the encrypted backdoor is located in a different directory (%Program Files%\Common Files\System\ado). This complex setup makes it harder to detect and remove all the backdoors, and is more effective at hiding any activities.

The complexity and the capabilities of these backdoors present a tough problem for the targeted organizations. It is a sophisticated attack that needs equally sophisticated security solutions.

Trend Micro Solutions

The Lazarus group is an experienced organization, methodically evolving their tools and experimenting with strategies to get past an organization's defenses. The backdoors they are deploying are difficult to detect and a significant threat to the privacy and security of enterprises, allowing attackers to steal information, delete files, install malware, and more.

These and other tools used by the Lazarus group can be mitigated by routinely scanning the network for any malicious activity to help prevent the malware from entering and spreading through an organization. In addition, educating employees and other key people in an organization on social engineering techniquesopen on a new tab can allow them to identify what to look out for when it comes to malicious attacks.

Other mitigation strategies include a multilayered approach to securing the organization's perimeter, which includes hardening the endpointsopen on a new tab and employing application controlproducts to help prevent malicious applications and processes from being executed.

Trend Micro endpoint solutions such as Trend Micro™ Smart Protection Suitesproducts and Worry-Free™ Business Securityworry free services suites can protect users and businesses from these threats by detecting malicious files and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™products has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs that could lead to malicious downloads.

Trend Micro XGen™products security provides a cross-generational blend of threat defense techniques to protect systems from all types of threats. It features high-fidelity machine learningopen on a new tab on gatewaysproducts and endpointsproducts, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen security protects against today's threats that bypass traditional controls; exploit known, unknown, or undisclosed vulnerabilities; either steal or encrypt personally identifiable data; or conduct malicious cryptocurrency mining. Smart, optimized, and connected, XGen security powers Trend Micro's suite of security solutions: Hybrid Cloud Securityproducts, User Protectionproducts, and Network Defenseproducts.

Indicators of Compromise

Command and Control Servers

107[.]172[.]195[.]20

192[.]3[.]12[.]154

46[.]21[.]147[.]161
