CLOUD SECURITY

LOLBins: Understanding the Silent Operations of Attackers

September 01, 2021

Share

Uptycs Threat Research

Tags Cloud Security Threats

Original research by Pritam Salunkhe and Shilpesh Trivedi

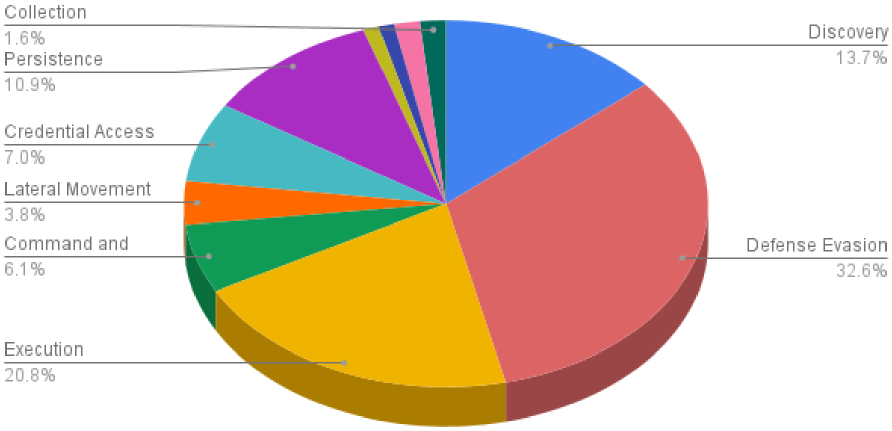
The Uptycs Threat Research team has observed several malicious binaries in our threat intelligence systems using LOLBins in their attack kill chain. LOLBins (short form for Living Off the Land Binaries), are non-malicious native operating system or known software binaries used for performing malicious activities and evading cyber defenses.

The Uptycs Threat research team has created over 300 rules covering different techniques used by LOLBins in the MITRE ATT&CK framework.

In this post, we'll take a look at the LOLBins used by the attackers and how you can use Uptycs EDR detection capabilities to find if these have been used in your environment.

Living off the Land binaries exploit the trusted utilities for achieving malicious objectives. They are mostly used by threat actors to stay under the radar and continue malicious activities undetected. In Windows, most of the malware families are taking leverage of LOLBins for a wide variety of phases in the attack kill chain.

Uptycs EDR has a robust coverage for all LOLBAS (Living off the Land Binaries and Scripts) techniques in the wild. Using the data from our customer telemetry and threat intelligence systems, the Uptycs Threat research team has created over 300 rules covering 8 different tactics used by LOLBins in the MITRE ATT&CK framework. The distribution of these rules with the techniques is shown below (see Figure 1).



Using the data from our in-house threat intelligence systems and customer telemetry, we created a monitoring dashboard of all observed LOLBins. From April 2021 through July 2021, we have observed 26 binaries mostly used as LOLBins by several malware groups. The prevalence of the malicious binaries using the LOLBins is shown below (see Figure 2).

These LOLBins were identified to be exclusively used in the Defense Evasion and Execution phase of the MITRE ATT&CK framework. The distribution of the different ATT&CK tactics used by the attackers leveraging Windows utilities from April 2021 through July 2021 is shown below (see Figure 3).

The table below describes these 26 LOLbins, along with their =MITRE ATT&CK mapping and a command line example.

LOLBin	MITRE ID	MITRE Tactic	Description	C

			execute malicious DLLs.	
rundll32.exe	T1218	Defense Evasion	Adversaries may use rundll32.exe to load malicious DLLs.	r ..
EQNEDT32.exe	T1203	Execution	Adversaries may exploit CVE-2017-11882 vulnerability in eqnedt32 for remote code execution in target system.	E

			parameter to launch other Windows utilities for further attack.	
powershell.exe	T1059	Execution	Adversaries may use powershell.exe to download payloads or execute malicious PowerShell-based tools or scripts.	F S c e S

attrib.exe	T1564	Defense Evasion	Adversaries may use attrib.exe to hide files for defense evasion on the target system.	" "

			execution of performing lateral movement in the target network.
schtasks.exe	T1053	Privilege Escalation	Adversaries may abuse schtasks.exe utility to initiate execution or repeat execution of malicious code .

netsh	T1546	Persistence	Adversaries may use netsh to gain persistence by executing helper DLL.	r (
Chrome.exe	T1105	Command and Control	Adversaries can spawn chrome.exe to download malicious files on the target system.	c h a

			to delete volume shadow copies to prevent system recovery.	
net.exe	T1562	Defense Evasion	Adversaries can use net.exe to stop services on the target system.	C s
mshta.exe	T1218	Defense Evasion	Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript.	r r r

cscript.exe	T1059	Execution	Adversaries may use cscript.exe to execute VB Scripts.	" x ". b

			download tools and payloads from remote systems into compromised systems.	
certutil.exe	T1140	Defense Evasion	Adversaries may use certutil.exe to encode/decode payload to thwart detections/analysis.	

wscript.exe	T1059	Execution	Adversaries may use wscript.exe to to execute VBA, VBS, JS files.	V "
msiexec.exe	T1218	Defense Evasion	Adversaries may use msiexec.exe to silently launch local or remote malicious MSI files.	r h k

			compile executables from downloaded C# code.	/ @
reg.exe	T1112	Defense Evasion	Adversaries may use reg.exe to query, add or modify Windows registry.	F \ \ / \ \

findstr.exe	T1552	Credential Access	Adversaries may search for unsecured credentials which are stored in files in	f

bitsadmin.exe	T1197	Defense Evasion	Adversaries may abuse bitsadmin (Bits job) to download malicious code	b N h r C

			kill processes or stop services.	
whoami.exe	T1033	Discovery	Adversaries may try to find current logged in user or verify privileges of the user using whoami.exe.	c f
tasklist.exe	T1057	Discovery	Adversaries may use tasklist.exe to enumerate running processes in the compromised system.	t s

			to execute malicious COM payloads.	/ (

July 2021, we identified the following:

- Most of the LOLBin alerts we have identified have been triggered via decoy macro documents.
- **regsvr32.exe and rundll32.exe** have the highest number of counts as these utilities. These utilities were used exclusively by Qbot and IcedID malwares from the beginning of January 2021, as detailed in our previous blog.
- We have also seen a significant number of Loki and Agent Tesla malware samples exploiting a Microsoft Equation Editor (EE) vulnerability in the EQNEDT32.

We will now cover interesting examples of LOLBins and their corresponding MITRE ATT&CK tactics.

LOLBin - Chrome.exe

Tactic: Command & Control

Hash: eae1b54ba4168e16e951fde291520078d8a5f8b98447cedf5663ae62b9069127

Chrome is the most commonly used browser by most users even though it is not a defaut Windows utility. During June 2021, our threat intelligence systems detected a document "Resume.docx '' which spawned a

The document used with chrome.exe to create a new window via command line argument '--new-window' to download the payload from onedrive.com as shown below (see Figure 4).

LOLBin - Schtasks.exe

Tactic: Privilege Escalation

Hash: 6c92ed33934d5a604f57aac4ff33252720354285291791bed88b6f3f15b9631d

Schtasks is used to create scheduled tasks which can be executed from time to time recurrently. We identified a document using schtasks for privilege escalation.

The Excel document we identified launches schtasks via command line to run the existing task named as SilentCleanup.This action is performed to bypass UAC and execute powershell commands in elevated mode as shown below (see Figure 5).

LOLBin - Csc.exe

Tactic: Defense Evasion

Csc.exe is an inbuilt utility located in the Microsoft.NET\Framework\<Version> folder under the Windows directory. The main purpose of this utility is to compile C# code. As the malicious code isn't compiled, the adversaries may be able to bypass the detection and analysis as it can also be named as legitimate looking documents.

We identified a word document named “contract.docm”, which launches powershell to download the uncompiled C# code. After download is complete, csc.exe compiles the same executable code on the fly as shown below (see Figure 6).

LOLBin - netsh.exe

Tactic: Persistence

Hash: 36b891924e7259d7b517a5f16a108e63aca927da3610b1dcb4dee79a4ccd2223

Netsh is a command-line scripting utility that allows you to display or modify the network configuration. Netsh also has an option to add helper DLLs to extend functionality of the utility.

The path of the DLL is also entered into Windows Registry at HKLM\SOFTWARE\Microsoft\Netsh. This allows adversaries to maintain persistence and the execution of the DLL would take place whenever netsh is launched.

Conclusion

The Uptycs Threat Research team continues to see an increase in the LOLBins used in various stages of the MITRE ATT&CK framework. As most of these utilities are often used for daily activities, it becomes a challenge for traditional security solutions that do not monitor process behavior.

Uptycs' EDR functionality with suspicious parent/child process relationships, correlation and Threat intelligence provides comprehensive detection and visibility to identify and detect LOLBins malicious activity generically.

Credits: Thanks to our Uptycs Threat Research team member *Rohit Bhagat* for maintaining and making enhancements with the threat intelligence portal for identifying the latest LOLBins attacks.

Recommended Content

2021, Q4 Quarterly Threat Bulletin

Growing Trend of Attackers Using Regsvr32 Utility Execution

Inside the WinRAR Vulnerability: Decoding & Bolstering Protection

Stay in the loop

Get regular updates on all things Uptycs—from product updates to expert articles and much more

SOC 2 Type II Certified

Container Security Competency
Security Software Competency
AWS Graviton Ready
Public Sector
AWS Marketplace Seller

CIS Benchmarks™ Certified

MITRE Engenuity ATT&CK Eval TURLA 2023

500 Technology Fast 500 2023 NORTH AMERICA Deloitte.

CNAPP Hybrid Cloud Security

Platform

Cloud Security Pricing

Solutions

Workload Protection

Posture Management

Vulnerability Management

Container & Kubernetes Security

Software Supply Chain

File Integrity Monitoring

Detection & Response

Asset Management

Compliance & Risk

By Platform

AWS

Microsoft Azure

Google Cloud

Integrations

Tools and Integrations

Why Uptycs

Why Choose Uptycs

About Us

Case Studies

Reviews

Compare Uptycs

Aqua

Lacework

Sysdig

CrowdStrike

Resources

Resources

Analyst Reports

Product Briefs

Blog

Video Hub

Threat Research Report Team

Whitepapers

E-books

Webinars and Events

Company

Careers

News

CSU

Support

Partners

Partner Program

Upward Partner Program