Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

uptycs

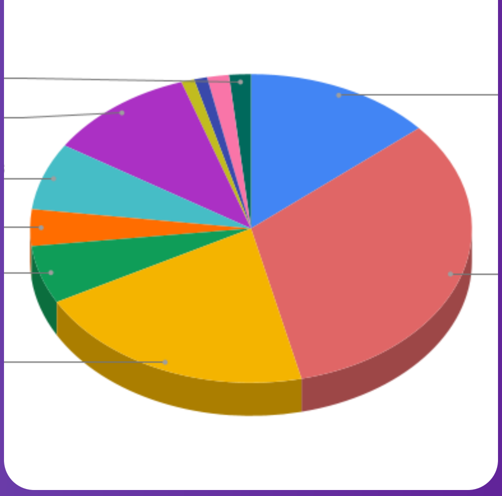
Platform Pricing Environments Why Uptycs Resources Partners Get demo

LOLBins: Understanding the Silent Operations of Attackers

September 01, 2021

CLOUD SECURITY

Share



Uptycs Threat Research

Tags Cloud Security Threats

Now Available

Gartner's 2024 CNAPP Market Guide

Analyst Report

Market Guide for Cloud-Native Application...

Download Report→

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.

Click here to see the LOLBins MITRE map

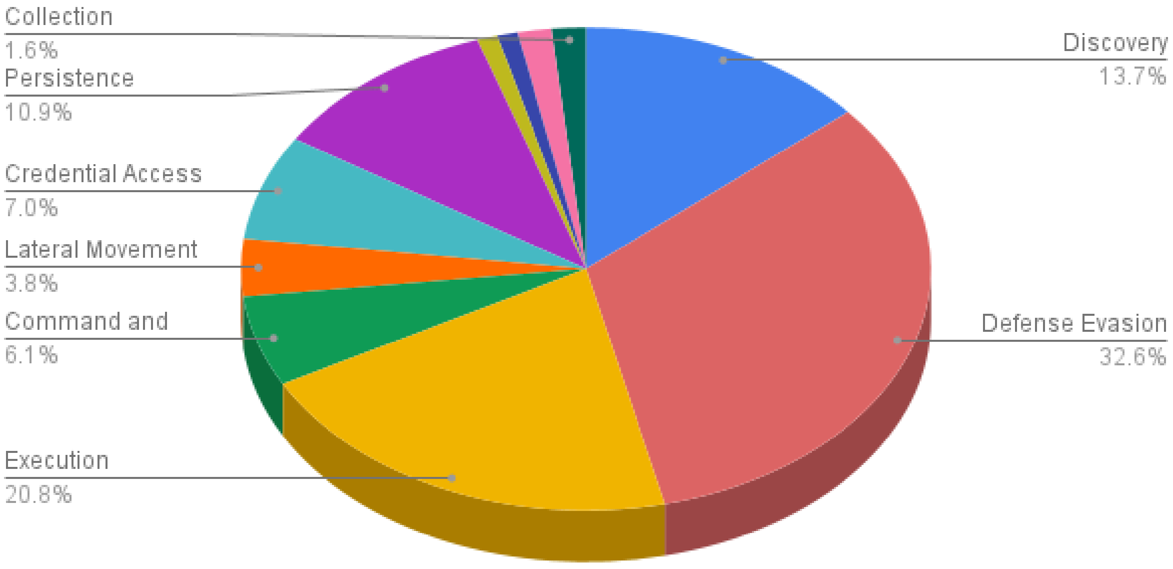
LOLBins & Uptycs EDR Coverage

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

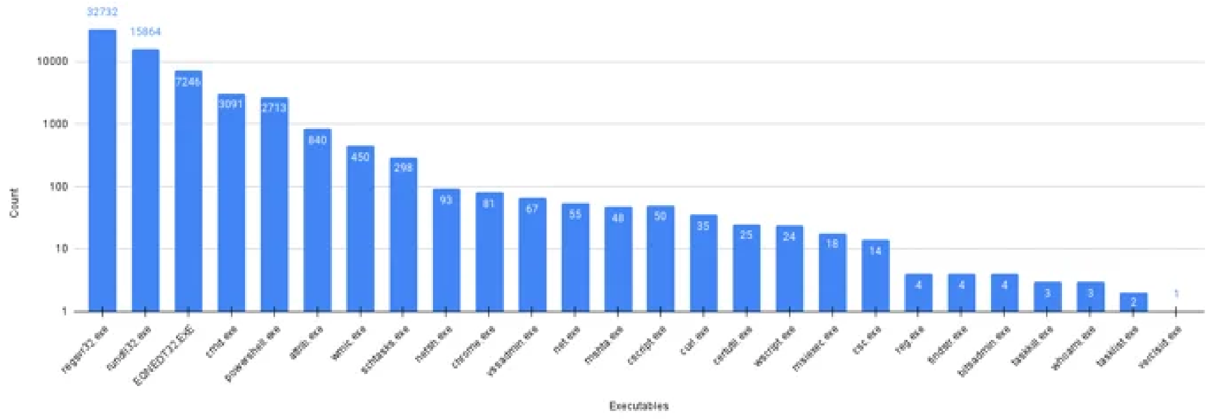
Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More →**



April - July 2021 LOLBins & MITRE ATT&CK Mapping

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).

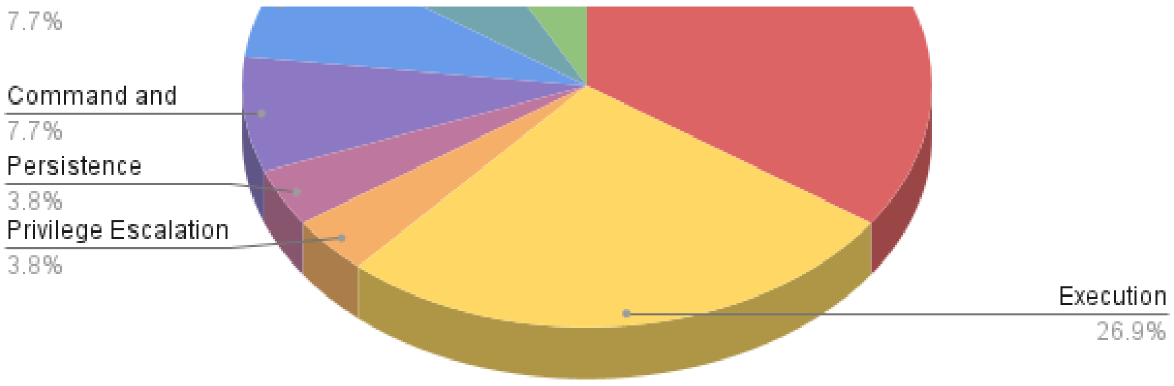
✕

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →



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
regsvr32.exe	T1218	Defense Evasion	Adversaries may use regsvr32.exe to execute malicious DLLs.	r
rundll32.exe	T1218	Defense Evasion	Adversaries may use rundll32.exe to load malicious DLLs.	r ..
EQNEDT32.exe	T1203	Execution	Adversaries may exploit CVE-2017-	E

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

			with /c or /k 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

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More →**

wmic	T1047	Execution	Adversaries may use wmic for execution or performing lateral movement in the target network.	v " C C
schtasks.exe	T1053	Privilege Escalation	Adversaries may abuse schtasks.exe utility to initiate execution or repeat execution of malicious code .	s \ p
netsh	T1546	Persistence	Adversaries may	r

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

			malicious files on the target system.	
vssadmin.exe	T1490	Impact	Adversaries may use vssadmin.exe to delete volume shadow copies to prevent system recovery.	v /
net.exe	T1562	Defense Evasion	Adversaries can use net.exe to stop services on the target system.	(s
mshta.exe	T1218	Defense Evasion	Adversaries may abuse mshta.exe to	r r

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

cscript.exe	T1059	Execution	Adversaries may use cscript.exe to execute VB Scripts.	x ". b
curl.exe	T1105	Command and Control	Adversaries may use curl.exe to download tools and payloads from remote systems into compromised systems.	c h p x

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

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
csc.exe	T1027	Defense Evasion	Adversaries may use csc.exe tool to compile executables from downloaded C# code.	" e x @

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

reg.exe	T1112	Defense Evasion	Adversaries may use reg.exe to query, add or modify Windows registry.	\ \ \ / \ \
findstr.exe	T1552	Credential Access	Adversaries may search for unsecured credentials which are stored in files in	f

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

			malicious code	
taskkill.exe	T1489	Impact	Adversaries may use taskkill.exe to kill processes or stop services.	t
whoami.exe	T1033	Discovery	Adversaries may try to find current logged in user or verify privileges of the user using whoami.exe.	c f

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

verclsid.exe	T1218	Execution	Adversaries may abuse verclsid.exe to execute malicious COM payloads.	v E / C

LOLBins Observations

Based on the data we obtained from April 2021 through July 2021, we identified the following:

- Most of the LOLBin alerts we have identified have been triggered via decoy macro documents.

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

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 new process of chrome.exe via command line. This activity often goes unnoticed by monitoring solutions.

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

Hash:
2048aae014930d195ac0c139c3260928bd25d840ff924fb46d25c79048a9c813

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won’t be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

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.

We identified an excel document that called wmic to create a new process of netsh to register the malicious DLL as the helper DLL as shown below (see Figure 8).

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.

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More** →

Recommended Content

2021, Q4 Quarterly Threat Bulletin

Growing Trend of Attackers Using Regsvr32 Utility Execution

WinRAR CVE-2023-38831 Vulnerability Draws Attention from APTs

Stay in the loop

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

email@work.com

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline

Achieve DORA Compliance with Uptycs: Securing Financial Services in the Cloud **Learn More →**

uptycs

Platform Pricing Environments Why Uptycs Resources Partners Get demo

AICPA SOC
SOC 2 Type II Certified

aws PARTNER
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.

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

Microsoft Azure

Google Cloud

Integrations

Tools and Integrations

About Us

Case Studies

Reviews

Compare Uptycs

Aqua

Lacework

Sysdig

CrowdStrike

Product Briefs

Blog

Video Hub

Threat Research Report Team

Whitepapers

E-books

Guides

Threat Quarterly Reports

Glossary

Webinars and Events

Company

Careers

News

CSU

Support

Program

Also of Interest MITRE Engenuity's ATT&CK Evaluations,... Uptycs blog Black basta Ransomware Goes Cross-Platform,...

© 2024 Uptycs. All rights reserved.

Privacy Policy Security Practices Contact Us

This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy

If you decline, your information won't be tracked when you visit this website. A single cookie will be used in your browser to remember your preference not to be tracked.

Accept Decline