TRUST DELIVERED

Ghosts in the Network

Uncovering APTs Like Hidden Cobra Without Clear Indicators of Compromise

SANS CyberFest Virtual Summit

November 2024

ReversingLabs At-A-Glance

40B+

Searchable Threat Repository

8X

Larger Than Nearest Competitor

60+

Cybersecurity Companies Trust RL

20M

Files Analyzed Daily

FASTEST

Software/File Deconstruction

3M

Malware Identified Daily

300

Employees Globally

CRN

5 Star Rated Partner Program

Gartner

Recognized for SSCS Solution

Verizon Business

DBIR

Report Contributor

Today’s Presenters

Stuart Phillips

Cyber Security Practitioner
ReversingLabs

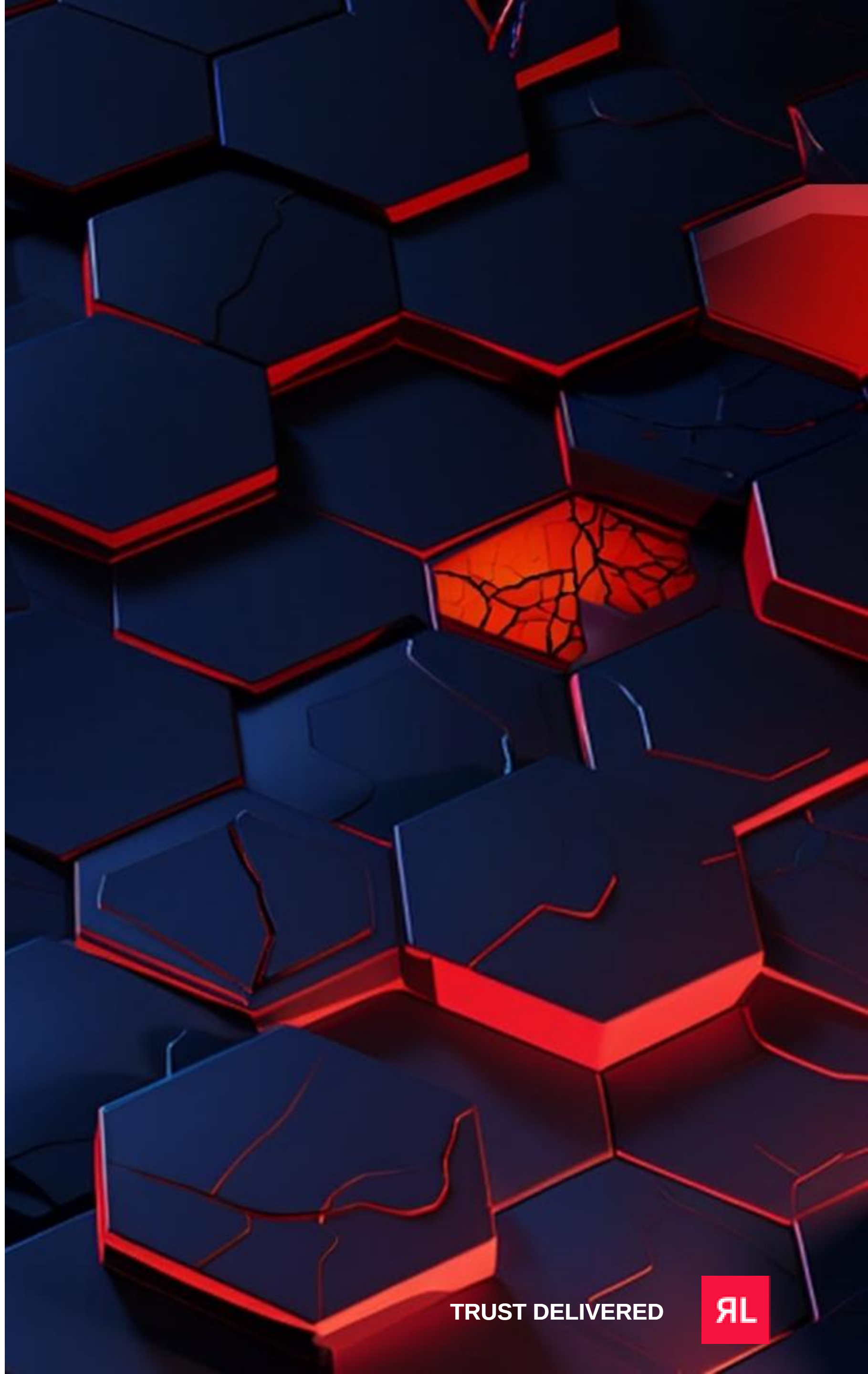
Ali N. Khan

Field CISO
ReversingLabs

This presentation is based on original research by ReversingLabs Threat Researcher, Karlo Zanki

Discussion Overview

- Who is Hidden Cobra (Lazarus)
- How to Read a Cyber Threat Report
- What are the current malware campaigns
- Spectra Analyze Overview
- Using Spectra Analyze to uncover malware
- Other methods to uncover malware
- Questions



TRUST DELIVERED

Who is Hidden Cobra (Lazarus)?

- Hidden Cobra, also known as Lazarus Group
- North Korean state-sponsored cyber threat group
- Notable Attacks: Sony Pictures Entertainment (2014), Bangladesh Bank heist (2016), WannaCry ransomware attack (2017)

How to Read a Cyber Threat Report

- Understanding Reports: Key components of a cyber threat report
- Interpreting Data: How to analyze and interpret threat data
- Actionable Insights: Turning report findings into actionable security measures

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea

Current Malware Campaigns

Recent and ongoing malware campaigns

- COPPERHEDGE, TAINTEDSCRIBE and PEBBLEDASH

Common tactics used by attackers

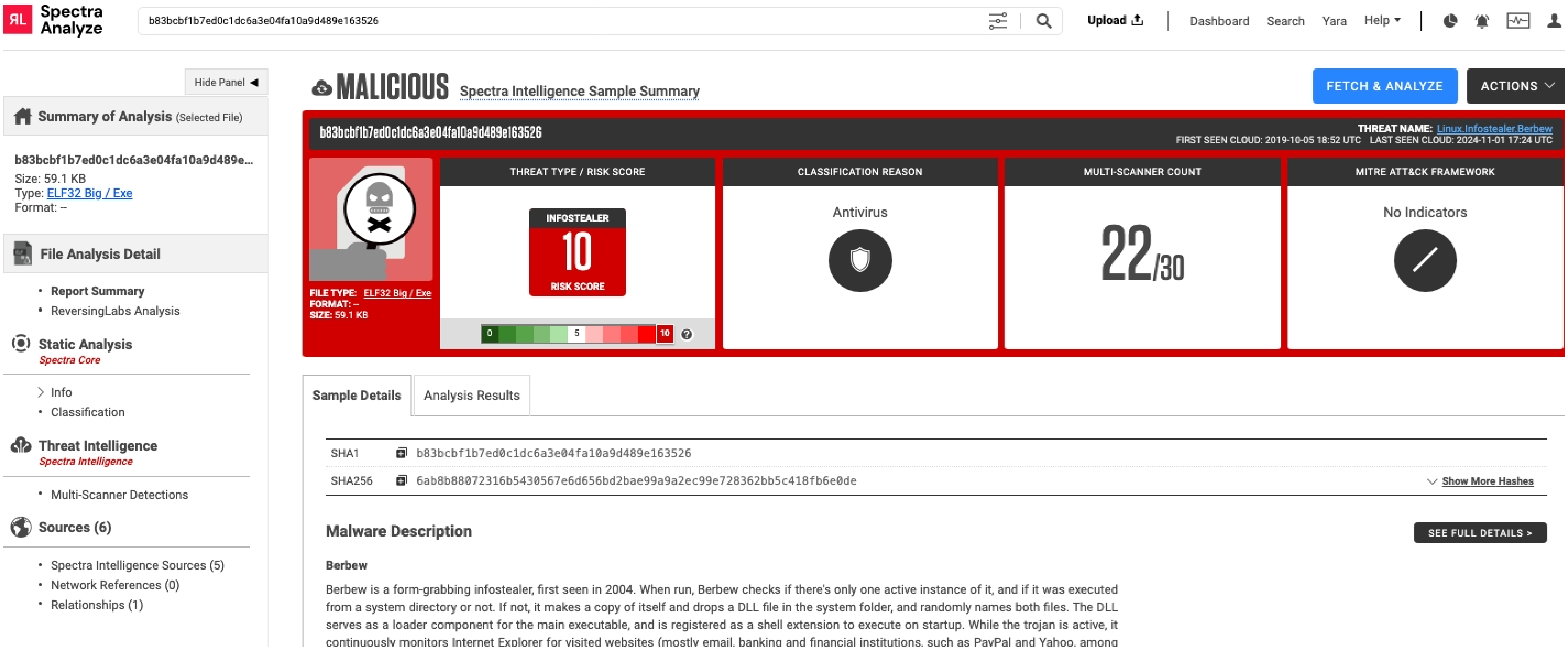
- Acquire Infrastructure
- Obfuscate Identity
- Purchase VPNs and VPSs
- Gain Access

Examples of recent malware campaigns

- Spear-phishing emails in targeted attacks against bank employees
- Windows-based malware to explore a bank's network to identify the payment switch application server
- Compromise payment server and coordinate with external ATM withdrawals

Spectra Analyze

- Spectra Analyze is instance-based appliance - Physical and Cloud
- Integration with many SOAR platforms



b83bcbf1b7ed0c1dc6a3e04fa10a9d489e163526

Summary of Analysis (Selected File)

b83bcbf1b7ed0c1dc6a3e04fa10a9d489e...
Size: 59.1 KB
Type: ELF32 Big / Exe
Format: –

File Analysis Detail

- Report Summary
- ReversingLabs Analysis

Static Analysis
Spectra Core

- Info
- Classification

Threat Intelligence
Spectra Intelligence

- Multi-Scanner Detections

Sources (6)

- Spectra Intelligence Sources (5)
- Network References (0)
- Relationships (1)

MALICIOUS Spectra Intelligence Sample Summary

b83bcbf1b7ed0c1dc6a3e04fa10a9d489e163526
THREAT NAME: Linux.Infostealer.Berbew
FIRST SEEN CLOUD: 2019-10-05 18:52 UTC LAST SEEN CLOUD: 2024-11-01 17:24 UTC

FILE TYPE: ELF32 Big / Exe
FORMAT: –
SIZE: 59.1 KB

THREAT TYPE / RISK SCORE	CLASSIFICATION REASON	MULTI-SCANNER COUNT	MITRE ATT&CK FRAMEWORK
INFOSTEALER 10 RISK SCORE 0 5 10	Antivirus	22/30	No Indicators

SHA1	b83bcbf1b7ed0c1dc6a3e04fa10a9d489e163526
SHA256	6ab8b88072316b5430567e6d656bd2bae99a9a2ec99e728362bb5c418fb6e0de

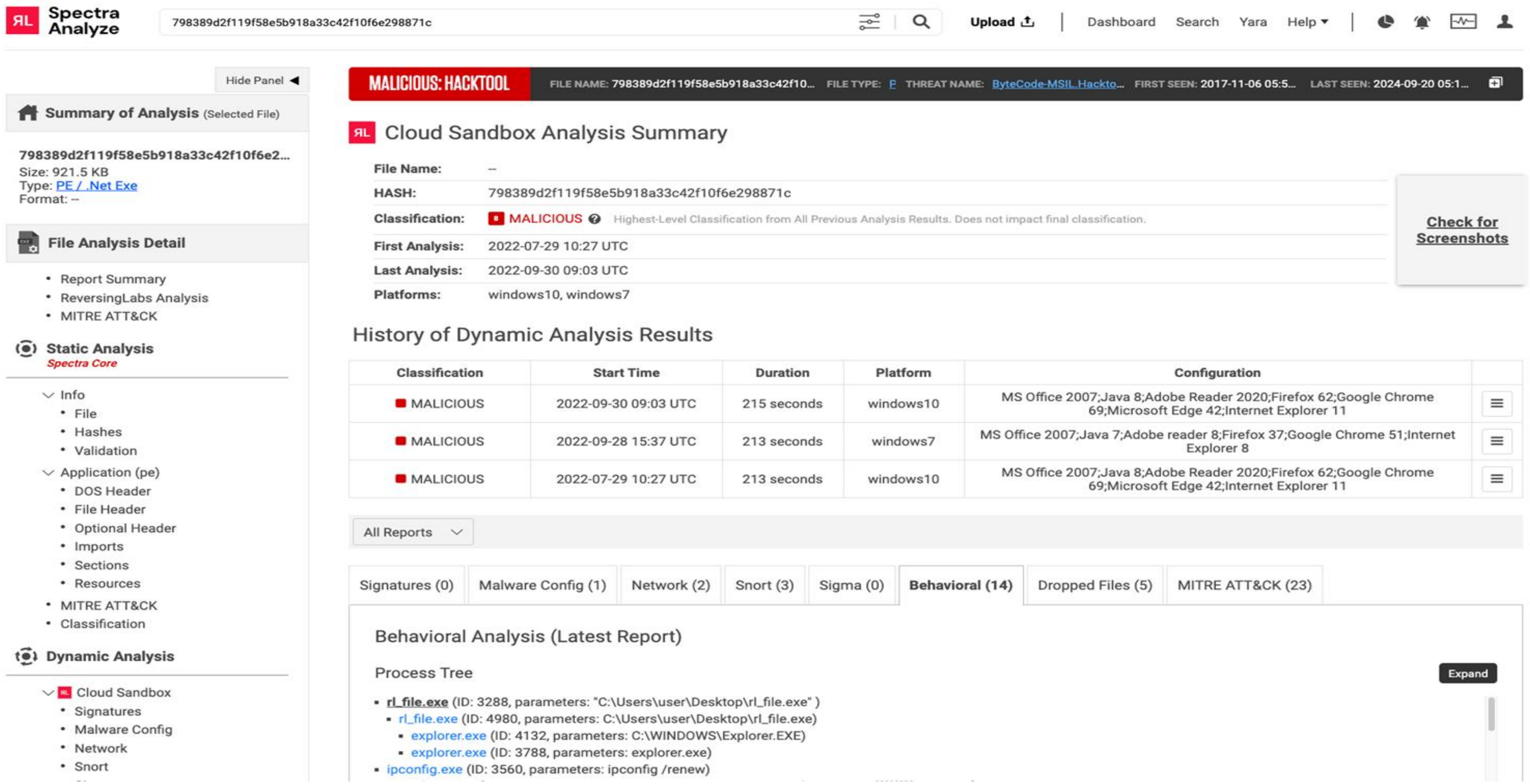
Show More Hashes

Malware Description

Berbew

Berbew is a form-grabbing infostealer, first seen in 2004. When run, Berbew checks if there's only one active instance of it, and if it was executed from a system directory or not. If not, it makes a copy of itself and drops a DLL file in the system folder, and randomly names both files. The DLL serves as a loader component for the main executable, and is registered as a shell extension to execute on startup. While the trojan is active, it continuously monitors Internet Explorer for visited websites (mostly email, banking and financial institutions, such as PayPal and Yahoo, among

Spectra Analyze Cloud Sandbox


Spectra Analyze
798389d2f119f58e5b918a33c42f10f6e298871c
Upload
Dashboard
Search
Yara
Help
Hide Panel
Summary of Analysis (Selected File)

798389d2f119f58e5b918a33c42f10f6e2...
Size: 921.5 KB
Type: PE / .Net Exe
Format: --

MALICIOUS: HACKTOOL FILE NAME: 798389d2f119f58e5b918a33c42f10... FILE TYPE: P THREAT NAME: ByteCode-MSIL.Hackto... FIRST SEEN: 2017-11-06 05:5... LAST SEEN: 2024-09-20 05:1...

Cloud Sandbox Analysis Summary

File Name:	--
HASH:	798389d2f119f58e5b918a33c42f10f6e298871c
Classification:	MALICIOUS Highest-Level Classification from All Previous Analysis Results. Does not impact final classification.
First Analysis:	2022-07-29 10:27 UTC
Last Analysis:	2022-09-30 09:03 UTC
Platforms:	windows10, windows7

Check for Screenshots

History of Dynamic Analysis Results

Classification	Start Time	Duration	Platform	Configuration
🟥 MALICIOUS	2022-09-30 09:03 UTC	215 seconds	windows10	MS Office 2007;Java 8;Adobe Reader 2020;Firefox 62;Google Chrome 69;Microsoft Edge 42;Internet Explorer 11
🟥 MALICIOUS	2022-09-28 15:37 UTC	213 seconds	windows7	MS Office 2007;Java 7;Adobe reader 8;Firefox 37;Google Chrome 51;Internet Explorer 8
🟥 MALICIOUS	2022-07-29 10:27 UTC	213 seconds	windows10	MS Office 2007;Java 8;Adobe Reader 2020;Firefox 62;Google Chrome 69;Microsoft Edge 42;Internet Explorer 11

Behavioral Analysis (Latest Report)

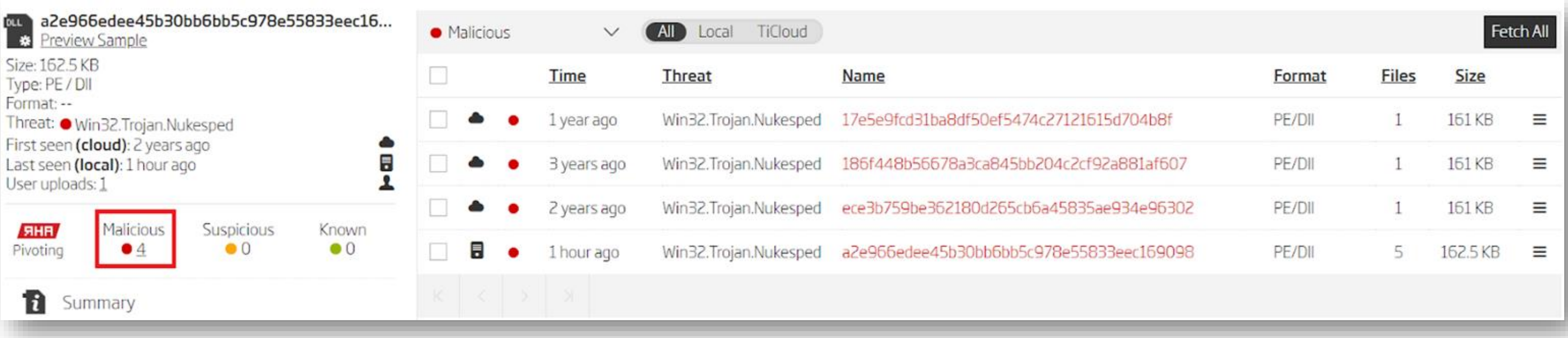
Process Tree

- rl_file.exe (ID: 3288, parameters: "C:\Users\user\Desktop\rl_file.exe")
  - rl_file.exe (ID: 4980, parameters: C:\Users\user\Desktop\rl_file.exe)
    - explorer.exe (ID: 4132, parameters: C:\WINDOWS\Explorer.EXE)
    - explorer.exe (ID: 3788, parameters: explorer.exe)
- ipconfig.exe (ID: 3560, parameters: ipconfig /renew)

Using Spectra Analyze to **Uncover Malware**

How do you uncover new malware without provided samples?

Use File Similarity ReversingLabs Hashing Algorithm (RHA)

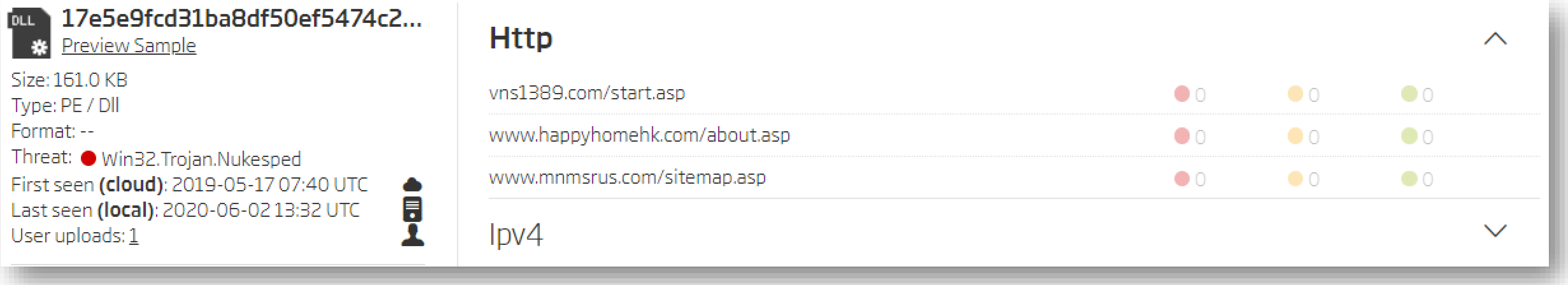


a2e966edee45b30bb6bb5c978e55833eec16...
Preview Sample
Size: 162.5 KB
Type: PE / Dll
Format: --
Threat: ● Win32.Trojan.Nukesped
First seen **(cloud)**: 2 years ago
Last seen **(local)**: 1 hour ago
User uploads: 1

□			Time	Threat	Name	Format	Files	Size	
□		●	1 year ago	Win32.Trojan.Nukesped	17e5e9fcd31ba8df50ef5474c27121615d704b8f	PE/Dll	1	161 KB	≡
□		●	3 years ago	Win32.Trojan.Nukesped	186f448b56678a3ca845bb204c2cf92a881af607	PE/Dll	1	161 KB	≡
□		●	2 years ago	Win32.Trojan.Nukesped	ece3b759be362180d265cb6a45835ae934e96302	PE/Dll	1	161 KB	≡
□		●	1 hour ago	Win32.Trojan.Nukesped	a2e966edee45b30bb6bb5c978e55833eec169098	PE/Dll	5	162.5 KB	≡

Using Spectra Analyze to **Analyze Malware**

Analyze Metadata within new samples to uncover new C2 domains



17e5e9fcd31ba8df50ef5474c2...

Preview Sample

Size: 161.0 KB

Type: PE / Dll

Format: --

Threat: ● Win32.Trojan.Nukesped

First seen **(cloud)**: 2019-05-17 07:40 UTC

Last seen **(local)**: 2020-06-02 13:32 UTC

User uploads: 1

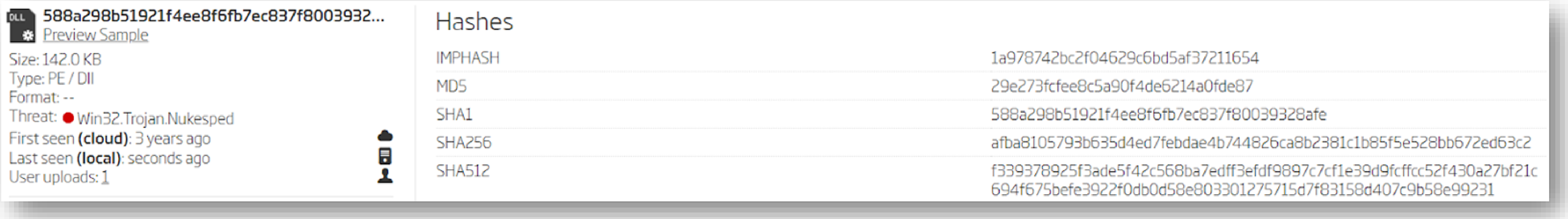
Http

vns1389.com/start.asp	● 0	● 0	● 0
www.happyhomehk.com/about.asp	● 0	● 0	● 0
www.mnmsrus.com/sitemap.asp	● 0	● 0	● 0

Ipv4

Using Spectra Analyze for **Section Hashing**

YARA Retro Hunt uncovers previously used codebase to uncover more malware

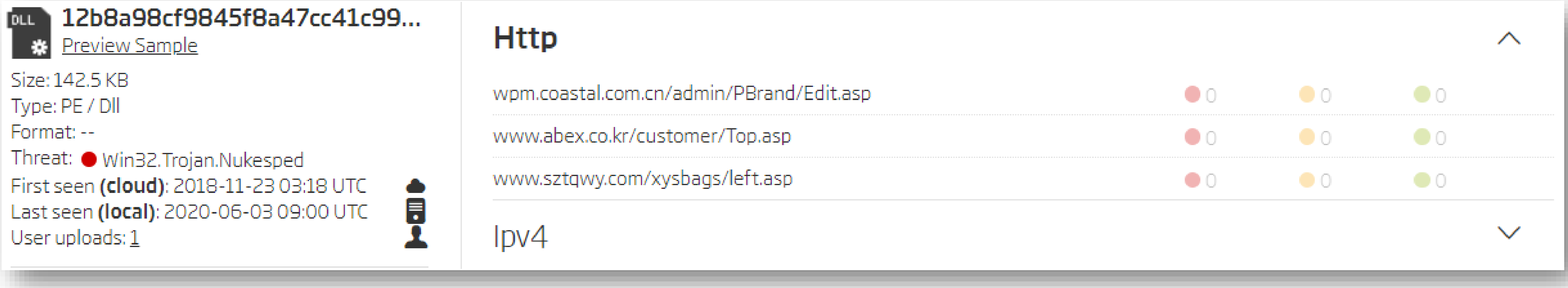


588a298b51921f4ee8f6fb7ec837f8003932...
Preview Sample

Size: 142.0 KB
Type: PE / Dll
Format: --
Threat: ● Win32.Trojan.Nukesped
First seen **(cloud)**: 3 years ago
Last seen **(local)**: seconds ago
User uploads: 1

Hashes

IMPHASH	1a978742bc2f04629c6bd5af37211654
MD5	29e273fcfee8c5a90f4de6214a0fde87
SHA1	588a298b51921f4ee8f6fb7ec837f80039328afe
SHA256	afba8105793b635d4ed7febdae4b744826ca8b2381c1b85f5e528bb672ed63c2
SHA512	f339378925f3ade5f42c568ba7edff3efdf9897c7cf1e39d9fcffcc52f430a27bf21c694f675befe3922f0db0d58e803301275715d7f83158d407c9b58e99231



12b8a98cf9845f8a47cc41c99...
Preview Sample

Size: 142.5 KB
Type: PE / Dll
Format: --
Threat: ● Win32.Trojan.Nukesped
First seen **(cloud)**: 2018-11-23 03:18 UTC
Last seen **(local)**: 2020-06-03 09:00 UTC
User uploads: 1

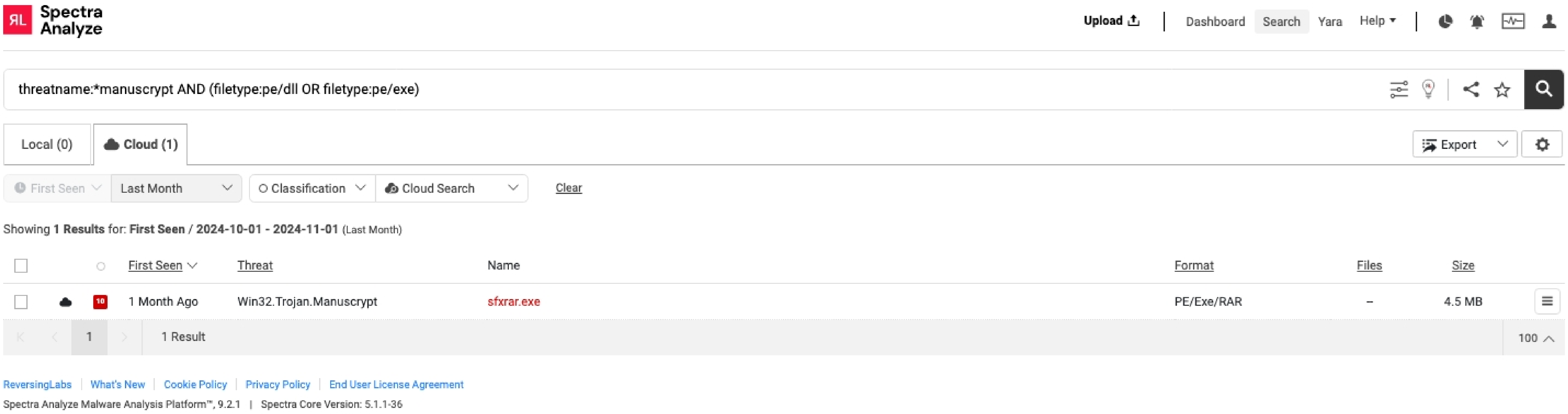
Http

wpm.coastal.com.cn/admin/PBrand/Edit.asp	● 0	● 0	● 0
www.abex.co.kr/customer/Top.asp	● 0	● 0	● 0
www.sztqwy.com/xysbags/left.asp	● 0	● 0	● 0

Ipv4

Using Spectra Analyze to **Deconstruct Malware**

Search by Threat Name (text within the files)



```
threatname:*manuscrypt AND (filetype:pe/dll OR filetype:pe/exe)
```

Showing **1 Results** for: **First Seen / 2024-10-01 - 2024-11-01** (Last Month)

First Seen	Threat	Name	Format	Files	Size
1 Month Ago	Win32.Trojan.Manuscrypt	sfxrar.exe	PE/Exe/RAR	–	4.5 MB

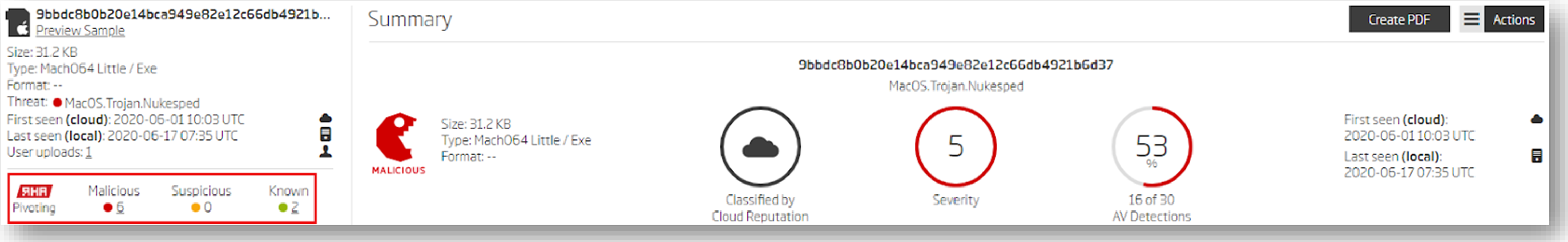
1 Result

100
ReversingLabs | What's New | Cookie Policy | Privacy Policy | End User License Agreement

Spectra Analyze Malware Analysis Platform™, 9.2.1 | Spectra Core Version: 5.1.1-36

Other Methods Using Spectra Analyze

- Search based on original file name
- Similar files grouped by RHA1 algorithm
- C2 domains used for TLS communication
- Files having similar file creation date



9bbdc8b0b20e14bca949e82e12c66db4921b...
Preview Sample

Size: 31.2 KB
Type: Mach064 Little / Exe
Format: --
Threat: ● MacOS.Trojan.Nukesped
First seen **(cloud)**: 2020-06-01 10:03 UTC
Last seen **(local)**: 2020-06-17 07:35 UTC
User uploads: 1

RHA Pivoting	Malicious	Suspicious	Known
	● 6	● 0	● 2

Summary

9bbdc8b0b20e14bca949e82e12c66db4921b6d37
MacOS.Trojan.Nukesped

MALICIOUS

Size: 31.2 KB
Type: Mach064 Little / Exe
Format: --

Classified by Cloud Reputation

5
Severity

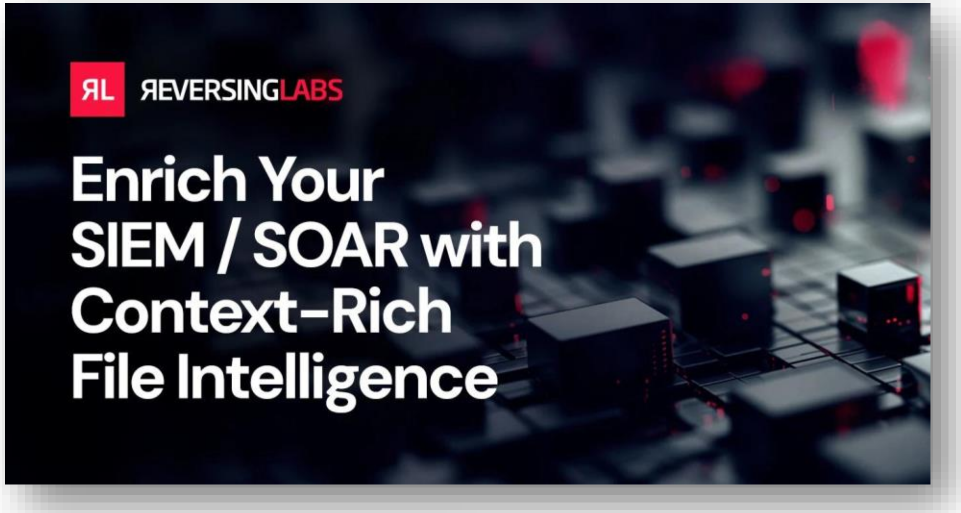
53 %
16 of 30 AV Detections

First seen **(cloud)**: 2020-06-01 10:03 UTC
Last seen **(local)**: 2020-06-17 07:35 UTC

QUESTIONS

https://www.reversinglabs.com/blog/hidden-cobra

Additional Insights & Events



Thank You