Tactics, Techniques and Procedures (TTPs) Utilized by FireEye's Red Team Tools

picussecurity.com/resource/blog/techniques-tactics-procedures-utilized-by-fireeye-red-team-tools

Keep up to date with latest blog posts

We have been routinely reading about new breaches this year, but this last incident is different from all others we have heard so far. FireEye, like all security vendors, fighting for a good cause. We support FireEye and we think that their response so far very mature and transparent sharing countermeasures to detect the use of their stolen tools.

We know that in such a situation and in a limited time, it is not easy to build all possible countermeasures. So we are also doing our best to support the community, sharing analysis, and additional countermeasures to help organizations to validate and improve their security posture for the possible use of the leaked Red Team tools against them.

Executive Summary

In this article, we analyzed 60 tools stolen from FireEye Red Team's arsenal to understand the impact of this breach. We found that:

- 43% of the stolen tools are publicly available tools that are using known attack techniques.

- 40% of tools are developed in-house by FireEye. These tools also utilize known adversary techniques.
- 17% of the stolen tools cannot be identified since FireEye did not share adequate details about these tools. According to their names, we believe that most of these unknown tools are also slightly modified versions of publicly available tools.

FireEye also announced that exploits of 16 vulnerabilities were also stolen. But there is no room for a big concern regarding these vulnerabilities and their exploits since they are already well-known.

At first, this breach remained the stolen NSA hacking tools published in the Shadow Brokers leak. A couple of high severity 0-day exploits were released in the NSA breach. These 0-day exploits caused severe security incidents worldwide, such as WannaCry and NotPetya. However, stolen tools and exploits in the FireEye breach utilizes known attack techniques. Our analysis shows that this breach will not have high impact on organizations.

Still, countermeasures should be taken against the stolen tools since they are frequently used by threat actors. In our new blog post, "It is Time to Take Action - How to Defend Against FireEye's Red Team Tools", we shared our comprehensive Blue Team recommendations, our detection contents as SIGMA and vendor-specific queries, and also vendor-based prevention signatures related to defending against FireEye Red Team tools.

Stolen Red Team Tools

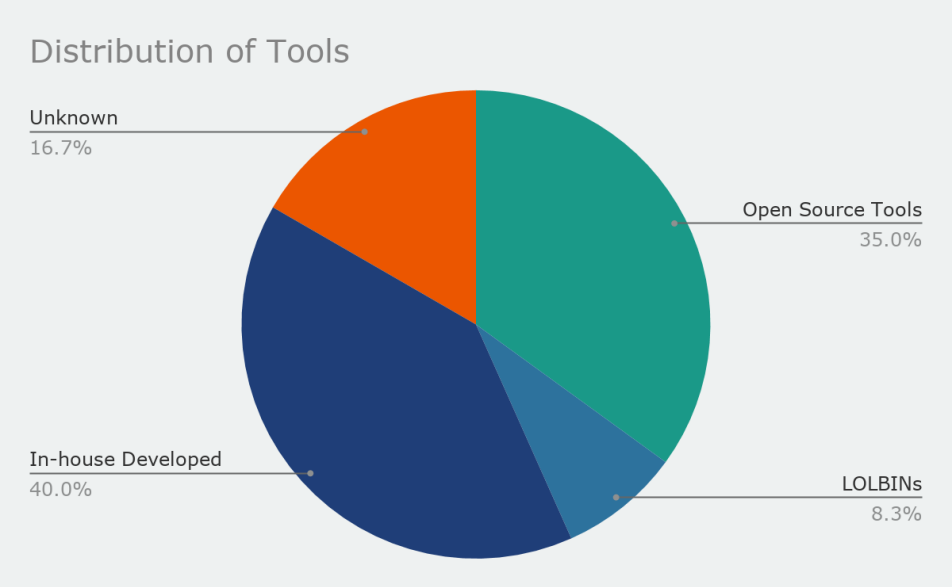
FireEye has not shared details about what the stolen red team tools do. The Red and Blue Team analysts of Picus Labs analyzed the compromised tools to reveal the functionalities and possible impacts of these tools.

We categorized these tools into four sets:

1. **Tools Based on Open Source Projects:** These red team tools are slightly modified versions of open-source tools.

2. **Tools Based on Built-in Windows Binaries:** These tools use built-in Windows binaries known as LOLBINs (Living Off The Land Binaries) [1].
3. **Tools Developed In-house for Fireeye's Red Team:** These tools are specially developed for the use of FireEye's Red Team.
4. **Tools Without Adequate Data to Analyze:** There is not enough data to analyze these tools. The Yara rules published by FireEye for the following tools are specific to ProjectGuid of the tool.

The below chart shows the distribution of stolen red team tools according to the above categories.



Stolen Exploits

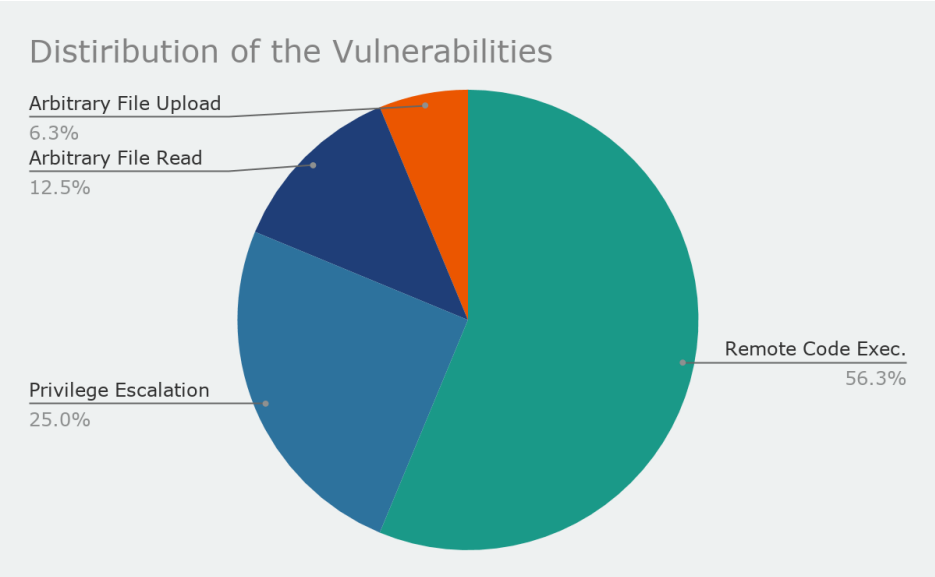
In addition to the red team tools, there are also exploit payloads affected by the incident. Leaked payloads exploit the following list of vulnerabilities. According to FireEye's report, leaked payloads do not include a 0-day exploit.

CVE Number	Vulnerability Type	Affected Product	CVSS	Picus ThreatID
CVE-2014-1812	Privilege Escalation	Windows	9.0	
CVE-2016-0167	Privilege Escalation	Microsoft Windows	7.8	
CVE-2017-11774	Remote Code Execution	Microsoft Outlook	7.8	

CVE-2018-13379	Pre-auth Arbitrary File Read	Fortigate SSL VPN	9.8	545960
CVE-2018-15961	Remote Code Execution	Adobe ColdFusion	9.8	
CVE-2019-0604	Remote Code Execution	Microsoft Sharepoint	9.8	365560 836508
CVE-2019-0708	Remote Code Execution	Windows Remote Desktop Services (RDS)	9.8	689860
CVE-2019-11510	Pre-auth Arbitrary File Read	Pulse Secure SSL VPN	10.0	575541
CVE-2019-11580	Remote Code Execution	Atlassian Crowd	9.8	
CVE-2019-19781	Remote Code Execution	Citrix Application Delivery Controller and Citrix Gateway	9.8	311195 321318
CVE-2019-3398	Authenticated Remote Code Execution	Confluence	8.8	541281
CVE-2019-8394	Pre-auth Arbitrary File Upload	ZoHo ManageEngine ServiceDesk Plus	6.5	
CVE-2020-0688	Remote Code Execution	Microsoft Exchange	8.8	765961
CVE-2020-1472	Privilege Escalation	Microsoft Active Directory	10.0	318083 474540
CVE-2018-8581	Privilege Escalation	Microsoft Exchange Server	7.4	
CVE-2020-10189	Remote Code Execution	ZoHo ManageEngine Desktop Central	9.8	752616
CVE-2014-1812	Privilege Escalation	Windows	9.0	

CVE-2016-0167	Privilege Escalation	Microsoft Windows	7.8	875573
CVE-2017-11774	Remote Code Execution	Microsoft Outlook	7.8	468843
CVE-2018-15961	Remote Code Execution	Adobe ColdFusion	9.8	764471
CVE-2019-11580	Remote Code Execution	Atlassian Crowd	9.8	
CVE-2019-8394	Pre-auth Arbitrary File Upload	ZoHo ManageEngine ServiceDesk Plus	6.5	
CVE-2018-8581	Privilege Escalation	Microsoft Exchange Server	7.4	

Below chart shows the distribution of the vulnerabilities according to the vulnerability type:



Usual Suspects

FireEye frequently engages with Russian threat actors being a cybersecurity company fighting with APT groups and nation-state threat actors. According to the Washington Post, APT29 (also known as YTTRIUM, The Dukes, Cozy Bear, and CozyDuke) [2] carried out the FireEye breach [3]. However, there is no evidence to prove that.

Update (December 14, 2020)

IT company SolarWinds announced on Sunday that the SolarWinds Orion network monitoring product has been tampered by a state-sponsored threat actor via embedding backdoor code into a legitimate SolarWinds library [31]. This leads to the attacker having remote access into the victim's environment and a foothold in the network, which can be used by the attacker to obtain privileged credentials. Today, SolarWinds breach is connected to the FireEye breach, and suspicions on Russia increased [32].

Blue Team Recommendations

Picus Labs' Blue Team prepared a list of recommendations for preventing and detecting the stolen tools and exploits.

1. **Mitigating Vulnerabilities**
   Assess your systems against vulnerabilities listed in the above section using vulnerability scanning and monitoring tools. If there are any gaps you haven't patched yet, you must fix them, and you should check if they have been abused in your systems.

2. **Compromise Assessment**
   You can conduct compromise assessments on your systems by using released Yara rules by FireEye [4]. To utilize Yara rules, you can use an open-source Yara scanning tool or enterprise product and distribute it to the endpoints on your systems, then add the rules and get the results. Moreover, you can use IoCs included in Yara rules and search them in your SIEM environment.

3. **Utilize IOCs**
   To prevent and detect future related threats, you can add IOCs given in this report to your security products, such as EDR, EPP, and SIEM. However, keep in mind that these IoCs can easily be changed by adversaries.

4. **Utilize Snort Rules**
   Most network security products support Snort rules. You can add released Snort rules to your security devices[4]. If you are already using Snort, you can check the current rules are up to date.

5. **Update Your Security Products**
   Security vendors are releasing new signatures and rule sets that include countermeasures against stolen tools. Update your security products and their rule and signature sets.

6. **Hunting with OpenIOC**
   FireEye released some countermeasures in the OpenIoC format. You can add these rules to your security devices by developing detection and hunting rules using IoC editors.

Fore more detailed recommendations and our detection contents as SIGMA and vendor-specific (ArcSight, Carbon Black, QRadar, and Splunk) queries, and also vendor-based (CheckPoint, Cisco, Citrix, Fortinet, F5, McAfee, ModSecurity, Palo Alto Networks, Snort, Trend Micro) prevention signatures read our new blog post, "It is Time to Take Action - How to Defend Against FireEye's Red Team Tools".

Picus in Action

The Picus Threat Library includes most of the stolen tools, and the Picus Mitigation Library contains actionable mitigation recommendations and detection rules. Picus Labs' Red Team and Blue Teams are working on missed tools and adding them and their techniques to our libraries.

So, our users have already assessed their cyber defense against most of the stolen red team tools and their attack techniques. And, they fixed the identified gaps using actionable recommendations provided by Picus platform.

Detailed Analysis of the Tools

1. ## Tools Based on Open Source Projects:

These red team tools are slightly modified versions of open-source tools.

1.1 ADPassHunt

It is a credential stealer tool that hunts Active Directory credentials. There are two remarkable strings in the YARA rule [5] of this tool: Get-GPPPasswords and Get-GPPAutologons. Get-GPPPassword is a PowerShell script that retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences (GPP) [6]. Get-GPPAutologons is another PowerShell script that retrieves passwords from Autologon entries that are pushed through GPP. These scripts are used as functions in the PowerSploit, which is an offensive security framework combining PowerShell modules and scripts [7]. You can read our blog post to find out more information on the OS credential dumping technique.

MITRE ATT&CK Techniques
T1003.003 OS Credential Dumping: NTDS

T1552.06 Unsecured Credentials: Group Policy Preferences

AdPassHunt IOCs

590bd7609edf9ea8dab0b5fbc38393a870b329de

29385446751ddbca27c26c43015be7ab0d548b895531fba9b03d612e53bd9ff0

1.2 Beacon

This red team tool is based on the CobaltStrike beacon. A beacon is a CobaltStrike payload used by adversaries for several goals, such as persistence, execution, privilege escalation, credential dumping, lateral movement, and Command and Control (C2) communication over HTTP, HTTPS, DNS, SMB, and TCP protocols [8]. According to countermeasures published by FireEye, the Beacon tool uses HTTP, HTTPS, and DNS beacons. The Beacon tool utilizes built-in Windows binaries, such as msbuild.exe, Microsoft.Workflow.Compiler.exe, and regsvr32.exe to execute arbitrary payloads, and searchindexer.exe for process injection to evade defenses. It renames these binaries to avoid name-based detection rules by masquerading. You can read our blog post to find out more information about the masquerading technique.

MITRE ATT&CK Techniques
T1071.001 Application Layer Protocol: Web Protocols

T1029 Scheduled Transfer

T1036.003 Masquerading: Rename System Utilities

T1036.004 Masquerading: Task or Service

T1036.005 Masquerading: Match Legitimate Name or Location

T1574.002 Hijack Execution Flow: DLL Side-Loading

T1047 Windows Management Instrumentation

T1072 Software Deployment Tools

T1059.003 Command and Scripting Interpreter: Windows Command Shell

CobaltStrike Beacon IOCs

03a8efce7fcd5b459adf3426166b8bda56f8d8439c070b620bccb85a283295f4
e4dd5fc22ff3e9b0fa1f5b7b65fb5dfeac24aab741eee8a7af93f397b5720f4a
d011a846badec24a48a50d1ab50f57d356b9dd520408cbb3361182f6f0489a1e
0a566a0ddbaf9975221fe842b9b77c4a8b5d71bb2c33e0a46da26deec90dcbea
61cd1311d2e4663b86b5a70c2aafd5af6b247a6ebf407170296e37aaf8c69392

Picus Threat Library

853411 CobaltStrike Beacon used by OceanLotus Threat Group .DLL File Download Variant-1

748618 CobaltStrike Beacon Hack Tool used in Military Themed Campaign .EXE File Download Variant-1

649065 CobaltStrike Backdoor Malware .EXE File Download Variant-1

655930 CobaltStrike Backdoor Malware used by OceanLotus Threat Group .EXE
File Download Variant-1

1.3 Beltalowda

Beltalowda is a red team tool based on an open-source utility, SeatBelt. SeatBelt conducts a variety of security-oriented "safety checks" from both offensive and defensive security viewpoints related to the host survey [9].

Beltalowda / SeatBelt IOCs

d80b7a31d68b5f483073ff7af0984c1090f6a493f84db7d3a301e3e35fdb4a56
7b7cbb1a62faf7e7a9ee1d0254c5681779b61abd3c9763b6588857c14cccdd9b
8f991317f1473fa8af3c3d6ade2551ddac01425db6e7b0c718b81c324c43730d
1d841ff51f8b5b08d7b4752cd498108d4b3f82864257dbd8e35b097c766f9e24
29054e2cad080a61db11a61791206ea939cbf79abee71c44fa0e7603dd168840
dea11a5bc6ff271e40e477d1645bdeb19454bdd8eac077e598ca56ee885fc06e
b89158aeac0e98f7cc2a6c3040ad2f57093bdb9064eab2c585c1250d5efa850e
00d1726e2ba77c4bed66a6c5c7f1a743cf7bb480deff15f034d67cf72d558c83
5cacbf4e84027cb3c0ec55940dddee6f4d368aae778d635003cb3013b547ede0
bb939544ac109ca674ee9de4d8b292f9b117c9c676ddab61d15a6e219ad3986c

Picus Threat Library
295245 Information Gathering from Browsers using Seatbelt

830665 Information Gathering from Browsers using Seatbelt Variant-2

346711 Information Gathering by using Seatbelt Variant-3

1.4 Dtrim

Dtrim is a modified version of SharpSploit, which is an open-source .NET post-exploitation library written in C# [10]. SharpSploit ported modules of PowerShell post-exploitation frameworks like PowerSploit and other tools such as Mimikatz.

Picus Threat Library
888666 Credential Dumping from Windows Vault by using PowerSploit

841093 Process Injection by using Powersploit's Invoke-DllInjection Function

853912 Credential Dumping via SharpSploit’s Mimikatz Script Attack Scenario

322981 Information Gathering Scenario using Sharpsploit

778874 Credential Dumping by using Sharpsploitconsole and Sharpcradle

430106 Credential Dumping by using SharpSploit Library (compiled by SharpGen)

1.5 EWS-RT

EWS-RT is based on an open-source PowerShell tool, RT-EWS [11], which is a couple of cmdlets leveraging EWS (Exchange Web Services) API to perform specific enumeration and exploitation tasks on Microsoft Exchange Servers including Office365 and on-premise servers.

1.6 Fluffy

Fluffy is a modified version of Rubeus, which is an open-source C# toolkit for raw Kerberos interaction and abuses [12]. Red teams use Rubeus for Kerberoasting attacks and extracting Kerberos tickets [13].

MITRE ATT&CK Techniques

T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting

Fluffy IOCs (SHA1)

8bebf19d54c749560301eaada2e92eb240501b8c

1.7 G2JS

G2JS (GadgetToJScript) is an open-source tool for generating .NET serialized gadgets that can trigger .NET assembly load and execution when deserialized using BinaryFormatter from JS, VBS, and VBA scripts [14]. G2JS was created mainly for automating Microsoft Windows Script Host (WSH) scripts weaponization during red team engagements.

MITRE ATT&CK Techniques

T1059.005 Command and Scripting Interpreter: Visual Basic

T1059.007 Command and Scripting Interpreter: JavaScript/JScript

G2JS IOCs (SHA256)

dcce258cc818febe2b888c8eee42aa95393b2fb4f1f2406330840ab8ad5c7d50
A3a8dedf82741a1997b17a44fbb1e5712ba3a5db11146519cf39281def9329a7

eed9402cb6fdc047b12f67493ba10970155a00086918eaad9542ab24096cc715

398afc4c33e00b26466abb87668e33be766dbbf4c493fe04d180a14d14a32fa3

da3bdb6b9348a8d9328e669c744d0f21a83937c31894245e3157121342efe52c

cdabbe815b7aafa94469b97fa3665137c4d5b2da4fdd7648ba2851cf2df214fc

f8c8bb2ac03cc2a037ddde4ad175aa05aa80277483fcdac42627fbdcc36f64ba

fd2e546faed7426c448d1a11d8e1d4b8a06b5148c9c8dfa780338fac2ab53c5b

0b8eab0a1961c52c141ac058c11e070d724d600cf903f2457c8ed189e7aae047

117b9c9127beaf2e3ce7837c5e313084fd3926f1ebf1a77563149e08347cb029

Picus Threat Library
423316 Command Execution by using .NET Serialized Gadgets
467980 GadgetToJSCript (FireEye) HackTool .TXT File Download Variant-1

1.8 ImpacketObf

ImpacketObf (ImpacketObfuscation) is a collection of obfuscated Impacket utilities. Impacket is an open-source collection of Python classes for working with network protocols [15].

1.9 ImpacketOBF (SMBExec)

This tool is based on Impacket's smbexec.py tool.

1.10 ImpacketOBF (WMIExec)

This tool is based on Impacket's wmiexec.py tool.

MITRE ATT&CK Techniques
T1047 Windows Management Instrumentation

1.11 InveighZero

InveighZero is an open-source spoofer and man-in-the-middle (MitM) attack tool designed to assist red teamers and penetration testers [16], [17]. It can spoof LMNR, NBNS, mDNS, DNS, and DHCPv6 protocols.

MITRE ATT&CK Techniques
T1557.001 Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay

InveighZero IOCs (SHA256)

78fafeb22bf31de02a4b56114e86dcc3394e382658a5c95b1a302d3d8794718d
2728c46f4fcf62f3faee72be30f1dd75528391b0d70da302544f5282d58c931b
715b415647f33937b39aa072001bfb9857a4bea884d009cbe0c27f1422b9f55b
452c6651e79d9f69a55e711c0b4d70eb2b1aaac206b8a274e45d22f9d7cafd2c
50c4f46e43d30c9520be35e294ef98d81f81d60602cd659367bbcf6a91766c0f
a66f3a9ddf9343aeed40276c1abfc485f089050074a03801cd9a16787a39c6bf
0c080548e15e7f377baed2a550d48a555e6150d969f7f4b8244c3b3a50afb858

Picus Threat Library
685789 Credential Access via Network Sniffing by using Inveigh

1.12 KeeFarce

KeeFarce is an open-source tool that extracts KeePass 2.x password database information from memory [16]. It uses DLL injection to execute code within the context of a running KeePass process.

MITRE ATT&CK Techniques
T1555.001 Process Injection: Dynamic-link Library Injection

KeeFarce IOCs (SHA256)

5ea9a04284157081bd5999e8be96dda8fac594ba72955adacb6fa48bdf866434

Picus Threat Library
206268 Credential Dumping by using KeeFarce

1.13 NetAssemblyInject

This tool injects C# .NET assemblies into arbitrary Windows processes. It is based on an open-source tool, NET-Assembly-Inject-Remote [18] .

Picus Threat Library
459538 Credential Dumping using NetAssembly Injection Tool

1.14 NoAmci

NoAmci is an open-source tool that uses DInvoke to patch AMSI.dll to bypass AMSI (Windows Antimalware Scan Interface) detections [19].

Picus Threat Library
422966 Disabling Security Tools by using NoAmci Tool (AMSI Bypass)

1.15 PuppyHound

PuppyHound is a modified version of an open-source tool, SharpHound [20]. It is the C# data collector for the BloodHound Project [21].

PuppyHound / SharpHound IOCs (SHA256)

23490f7ac40b6b15c228ed8f8e9122d460469aa4025ed7008660e4310ef7e70f
a7240d8a7aee872c08b915a58976a1ddee2ff5a8a679f78ec1c7cf528f40deed
5fabe36fb1da700a1c418e184c2e5332fe2f8c575c6148bdac360f69f91be6c2
7b0a7e5d344f8ffa1a097cd9e658ecaa551fd84cfcc92a5fe46f9965661662cc
e9e646a9dba31a8e3debf4202ed34b0b22c483f1aca75ffa43e684cb417837fa
a07002c5d7712e751dfbcab1f05190793eb417b693b61f8ba0750fa15f88f61b
0d9fbc16c6f316d8ee1b9ff47b300c24a1964fdfc3990b680d05dab5e1905d9f
ee72671628902e2cd75fde74b7926355b39d1ab50be0aa8bc06e8f06344fc22c
36d4e69106bc8530d7923442d1929558b876f7f10545316623ae3db1b93ec584
e333444d815055181402f5fdbf60a62c4545e64f3e382c7685b47b7b5a6c27e8

Picus Threat Library
273197 Domain Information Discovery by using SharpHound

1.16 Rubeus

Rubeus is an open-source C# toolkit for raw Kerberos interaction and abuses [12]. Red teams use Rubeus for Kerberoasting attacks and extracting Kerberos tickets [13].

MITRE ATT&CK Techniques

T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting

Rubeus IOCs (SHA256)

a729d51f3deff5065e4978df2f88517d26e0d5db542c9cf8501a4206d8d2432c
9758688dd18db6ec86c4835d9ba67b5e209c32c81981dc69d705670f8b95d5e6
0340043481091d92dcfb2c498aad3c0afca2fd208ef896f65af790cc147f8891
76faeb790d1c1aa5fd3473f86f602b371682415368ddd553ebc60eb3c7683f7f
0097d59dc02cbac14df25ef05fc6d75f835d1db68f760d71fa4a0a57d9960606
c74352729dd49829f5e398a7fc7dd033d9e4aba3d93162c4fbcbe394cc31c3d4
9c6a910a047e29e07b4015866dc05e00829b888a86d1d357ed49652a9b73f1b6
6c1829be1c49c04b956b431386c389a6bf83327a5e7e68ff453103820ad4464d
817867c23a7bf47e99c93201f99f5eb805396327765aa76338c5f9e0c89eac4a
65044ea9fea1e34042adf3ff5e5fb17fc021ba4b0775415fad2465558a782c5e

Picus Threat Library
471775 Pass the Hash by using Rubeus Tool with asktgt Module (Pass The Key)

479855 Kerberoasting Attack by using Rubeus Tool

217117 Kerberoasting Attack by using Rubeus Tool Variant-2

893519 Pass the Hash by using Rubeus Tool (1.5.0) with asktgt Module (Pass The Key)

789965 Kerberoasting Attack by using Rubeus Tool (1.5.0)

509384 AS-REP Roasting Attack by using Rubeus Tool

1.17 SafetyKatz

SafetyKatz is a combination of Mimikatz and .NET PE Loader [22]. It creates a minidump of LSASS and uses PELoader to load a customized version of Mimikatz for credential dumping.

MITRE ATT&CK Techniques
T1003.001 OS Credential Dumping: LSASS Memory

SafetyKatz IOCs (SHA256)

2b3cab071ca6f104377a7684eb586150fdec11df2dc8cebcb468f57a82f10c73
89a456943cf6d2b3cd9cdc44f13a23640575435ed49fa754f7ed358c1a3b6ba9
3547d857af012c643a75bd3c1d3226c98e8181dc6e92872eb0746b26f6cc1a09
d1d3b00e8be37b30abfe2ff2aca90073ae517a27635a9fbb2e222981cf1ae817
796f70f7e01257c5b79e398851c836e915f6518e1e3ecd07bcd29233cf78f13d
bcf1857fe1eb566c0dbd032f7ec186bc1a31895861ac36887ad034501794fd00
4542ebba83ef6e16db6dc30383614bf52cb7c3f2fbd1577de10f02d6bf7dfc50
291a6968a3f7f2092c656d0275c604182d6f7ee7b813460aeb8b28c06d804b5e
b0a55532654bbfd0aafa59dfe26b576a095d9ac4a4af2f99bca442a1d87ce29b
27dd261ad7f3ad7d782625c2a459caf6ae81109ffe8f830b68b154f02d578658

Picus Threat Library
416382 Credential Dumping by using SafetyKatz Tool

549536 Credential Dumping by using SafetyKatz Tool Variant-2

764801 Mimikatz Execution with Evasion by using BetterSafetyKatz

779384 Credential Dumping using SafetyKatz Tool with AmsiScanBufferBypass

1.18 SharpUtils

It is an open-source collection of red team utilities written in C# language [23].

1.19 SharpZeroLogon

It is an open-source exploit for the Zerologon vulnerability (CVE-2020-1472) [24]. It exploits the cryptographic vulnerability in Netlogon to bypass authentication.

SharpZeroLogon IOCs (SHA256)

c4a97815d2167df4bdf9bfb8a9351f4ca9a175c3ef7c36993407c766b57c805b
b9088bea916e1d2137805edeb0b6a549f876746999fbb1b4890fb66288a59f9d
24d425448e4a09e1e1f8daf56a1d893791347d029a7ba32ed8c43e88a2d06439
7a05fd67e9344d27c90a7196ab32cbaf1ee8c14f8655e87cc3ebddca7eacebdf
eec19dd96f08c4b6c61e079cbff058bb79d928a3c3dd01b397222a3f5bfe2dd9
fa032802537b61f0e5f3645229a0758114b0c00ddc95273efba7a17ed18e2e00
10ed27a6dad3793933262c0a0b4ec1837c7127cde872acf23e4c42a8ecfd9109
7bcf833ab795b3a2cbd5df2e8caf5d664534b4623d0864dda73222dc47c56ec7

Picus Threat Library
792844 Exploitation of Zerologon Vulnerability via SharpZeroLogon Tool

1.20 TitoSpecial

TitoSpecial is based on an open-source tool AndrewSpecial, which is a credential stealer. It dumps credentials from LSASS memory. We explained this technique in our Credential Dumping blog.

MITRE ATT&CK Techniques
T1003.001 OS Credential Dumping: LSASS Memory

TitoSpecial / AndreSpecial IOCs (SHA256)

7bcf833ab795b3a2cbd5df2e8caf5d664534b4623d0864dda73222dc47c56ec7

Picus Threat Library
797345 TitoSpecial (FireEye) Infostealer .EXE File Download Variant-1

1.21 TrimBishop

This tool is based on an open-source tool, Rural Bishop [25].

TrimBishop / RuralBishop IOCs (SHA256)

38e7e5250287542688b12e216d9b25388061decde2f7255969a7a914cda0faf4
60247aa54635a0788f636aeab9752cc4e83ba4ae3ec336f60e01ab8dec856a05
7127e4b634f2bf6b9965d183c3dd61540ed4e08c4d60123da44892cf509cfe94
f821c3b8274d69e6948dea823682d16be0b23da3ea5363d6ffa0ea05e8654c05
b40c8fcb20acf66db418078f0d6099145b220dc056d095beb54665faf6c726c7

Picus Threat Library

754289 TrimBishop (FireEye) RAT .EXE File Download Variant-5

451090 TrimBishop (FireEye) RAT .EXE File Download Variant-4

854677 TrimBishop (FireEye) RAT .EXE File Download Variant-3

759601 TrimBishop (FireEye) RAT .EXE File Download Variant-2

746754 TrimBishop (FireEye) RAT .EXE File Download Variant-1

2. **Tools Based on Built-in Windows Binaries**

These tools use built-in Windows binaries known as LOLBINs (Living Off The Land Binaries) [1].

2.1 DueDLLigence

DueDLLigence is a shellcode runner framework previously published by FireEye[26]. Red Teams use it for application whitelisting bypass and DLL side-loading. It utilizes built-in Windows binaries Control.exe (Windows Control Panel), Rasautou.exe (Remote Access Dialer), and msiexec.exe (Microsoft Installer Executable) to bypass applications.

MITRE ATT&CK Techniques

T1218.002 Signed Binary Proxy Execution: Control Panel

T1218.007 Signed Binary Proxy Execution: Msiexec

DueDLLinge IOCs (SHA256)

9ff0c4211b7e0b6b9789c4a8576a5e2d1085ca729047a97518f46073ba558956
bcbc2f9367a909de763dca4d46d8328b65593df72abb5e61d2b8b104245f4814
df50e66c9f384a5ff9e3b23272677f3cc2962759947bffbfb905a12f21fd7a3d
71227bc1534a092ba03e6374cad929b193d1f6667cb781efd059b7d7d8e09c1d
aac1cd7e70f87d29504a017c7c1fe4ad276980d624d1f3651565cada52a37031

Picus Threat Library
590774 Dism.exe OS Binary (Lolbas) used in Signed Binary Proxy Executio

288390 DueDLLigence (FireEye) RAT .DLL File Download Variant-4

380893 DueDLLigence (FireEye) RAT .DLL File Download Variant-3

664528 DueDLLigence (FireEye) RAT .DLL File Download Variant-2

755632 DueDLLigence (FireEye) RAT .DLL File Download Variant-1

2.2 MSBuildMe

This red team tool is based on the MSBuild (Microsoft Build Engine), which is a platform for building applications [27]. It is used to compile and execute code and bypass the Application Whitelisting (AWL).

MITRE ATT&CK Techniques

T1127.001 Trusted Developer Utilities Proxy Execution: MSBuild

Picus Threat Library
422325 Microsoft Build Engine (MSBuild) Attack Scenario

395873 Parent PID Spoofing using APC Queue Code Injection

817545 Mimikatz Execution using MSBuild Task Property

2.3 NetshShellCodeRunner

This tool is based on Netsh.exe, which is a Windows tool used to manipulate network interface settings. Netsh.exe is used by adversaries and red teamers to execute a .dll file.

MITRE ATT&CK Techniques

T1546.007 Event Triggered Execution: Netsh Helper DLL

2.4 Uncategorized

This is a collection of tools that utilize built-in Windows binaries dism.exe, searchprotocolhost.exe, and werfault.exe for Process Injection.

MITRE ATT&CK Techniques

T1055 Process Injection

2.5 Weaponize

This tool uses the built-in Windows binary TSTheme.exe (TSTheme Server Module).

3. **Tools Developed In-house for Fireeye's Red Team**

These tools are specifically developed for the use of FireEye's Red Team.

3.1 DShell

DShell red team tool is a backdoor written in the D programming language. Its payload is encoded in Base64 format. According to Windows functions used by DShell, we guess it uses the process injection technique to inject its payload into a legitimate process.

DShell IOCs (SHA256):
747941f972e786f9a93c809247dc776d1fe348e004b1c087683756ae48acfdfe
4647ead22996882f3e1710404060547330 9f460d4f8d00f07395de89d81a039c
a6834eb32f20a52786ce1c5e99b94baec4d251414a97ca4717b2b06c88340a4b
2b4d48aac9c6885f50f5f95c10385aa10f7de9c8f393e64777b544e8fae8c95b
5e53ce8f7f5f0b9c85bcb15becc5ae4ce9f8fc01504e76deaafbf70ffa1cda9d
6500e845c478dc26d950b913da2fb85d6b180275827737062f23c8671b2cbd0e
c32514711f72002e9a540c2434dee7b239485d01a95a7530b939fed43f277f6d
77dedb037985896646ee3a65687dca17f669750133893209ea765c991a2c39a0
0c55581575708818bd5b58cd9647f1112f97a921f36227d4fe512e710e0a0dbf
225d4be8f66361b82dd89fc14496a1ebe37049c1930672dde2ccb6aab068aff1

Picus Threat Library

679074 DShell (FireEye) Backdoor .EXE File Download Variant-4

820177 DShell (FireEye) Backdoor .EXE File Download Variant-3

657835 DShell (FireEye) Backdoor .EXE File Download Variant-2

565235 DShell (FireEye) Backdoor .EXE File Download Variant-1

3.2 Excavator

This red team tool can dump a process directly or via its service. It is used by red teams to dump credentials from LSASS memory. You can read our Credential Dumping blog to learn the details of this technique.

MITRE ATT&CK Techniques

T1003.001 OS Credential Dumping: LSASS Memory

Excavator IOCs (SHA256):

efb533249f71ea6ebfb6418bb67c94e8fbd5f2a26cbd82ef8ec1d30c0c90c6c1
27a5e3795e150eb9d3af99a654be7d9a684983c0bbccc9ba0b4efa4301404760
31d06aa9ceb13c28b6af76d6b5cc33dc14c59e4496c9265cee60cbad3d89b863

3.2 Excavator

Excavator IOCs (SHA256) kutusu altına:Picus Threat Library

470104 Excavator (FireEye) Infostealer .DLL File Download Variant-1

Picus Threat Library

624090 Excavator (FireEye) Infostealer .DLL File Download Variant-2

244487 Excavator (FireEye) Infostealer .EXE File Download Variant-1

470104 Excavator (FireEye) Infostealer .DLL File Download Variant-1

3.3 GetDomainPasswordPolicy

It is a reconnaissance tool that obtains the password policy for an Active Directory domain.

3.4 GPOHunt

It is a reconnaissance tool that retrieves Group Policy configurations.

3.5 KeePersist

It is a tool developed in-house for Fireeye's Red Team that is used for persistence.

3.6 LNKSmasher

LNKSmasher is a tool that generates malicious .LNK files. LNK is a file format used for shortcut files that point to an executable file. This red team tool can embed an arbitrary payload in an LNK file.

MITRE ATT&CK Techniques

T1547.009 Boot or Logon Autostart Execution: Shortcut Modification

T1204.002 User Execution: Malicious File

3.7 LuaLoader

LuaLoader is a red team tool that can load arbitrary codes written in the Lua language. It is a tool developed in-house for Fireeye's Red Team.

3.8 Matryoshka

Matryoshka is a tool written in the Rust programming language. It is a multi-stage tool. After downloading the first-stage payload, it runs the second-stage malware via its dropper and installs the real payload. It uses the process hollowing technique [28] to evade defenses.

3.9 MemComp

The MemComp tool is used for in-memory compilation.

3.10 MOFComp

MOFComp (MOF Compiler) is a built-in Windows tool that parses a file containing MOF (Managed Object Format) statements and adds the classes and class instances defined in the file to the WMI (Windows Management Instrumentation) repository [29].

MITRE ATT&CK Techniques

T1546.003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

3.11 PGF

PGF is a backdoor development framework that utilizes several LOLBINs, such as Netsh, InstallUtil, Regasm, RunDLL32, Control, and Cstmp.exe.

MITRE ATT&CK Techniques

T1218.001 Signed Binary Proxy Execution: Compiled HTML File

T1218.002 Signed Binary Proxy Execution: Control Panel

T1218.003 Signed Binary Proxy Execution: CMSTP

T1218.004 Signed Binary Proxy Execution: InstallUtil

T1218.005 Signed Binary Proxy Execution: Mshta

T1218.007 Signed Binary Proxy Execution: Msiexec

T1218.008 Signed Binary Proxy Execution: Odbcconf

T1218.009 Signed Binary Proxy Execution: Regsvcs/Regasm

T1218.010 Signed Binary Proxy Execution: Regsvr32

T1218.011 Signed Binary Proxy Execution: Rundll32

T1216.001 Signed Script Proxy Execution: PubPrn

T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control

T1036.005 Masquerading: Match Legitimate Name or Location

T1055 Process Injection

T1574.002 Hijack Execution Flow: DLL Search Order Hijacking

T1574.002 Hijack Execution Flow: DLL Side-Loading

PGF IOCs (SHA256)

1208a9fcee5cf7522676427a7b8ceb6d49f7fcb6295f759b8cda0c3b3066a7e1
a0d5f287b9b3c0f540d5a59db423b86776a81181f81e14082d7b72ac1d99f8ea
86313ef291ebc5905837f16a8a99992550f986feca21fdc40f554b674c7298f7
1a9d041c82423805bc01b4cb1f5c20c5d58ebc4b525fd88553803a2f148ebd8d
ebc16780fe7083af5a9e143b56e0a791115f8b37b83f1bad5bab4828623e1224
032d1aa450227df5d23cc304009ad2db48b33e78191f464a1acc101807845aa7
65e7006479b5be1d094047a201da9a83e3ed424835752c62534bac32a9f3153b
24e37e197bdbabf8a2bc63e0776e82c00a440febe171ec1e648f024338c0871c
e1a42ea65004088638bd06353c14f85dcb0030e9fb6975425c6916d8f4f36dd3
304ee129a947706c6436d89215034332554cbb30cde833ce1d368d5b4b97eb3b

Picus Threat Library

573139 PGF (FireEye) Hacking Tool .EXE File Download Variant-3

819174 PGF (FireEye) Hacking Tool .EXE File Download Variant-2

674310 PGF (FireEye) Hacking Tool .EXE File Download Variant-1

3.12 PXELoot

It is a red team tool that discovers and exploits misconfigurations in Windows Deployment Services (WDS).

3.13 RedFlare

RedFlare is a Trojan development framework that includes builder, controller, downloader, and keylogger. It can generate Trojans for Windows and Linux systems.

RedFlare IOCs (SHA256):

037a51ea69153ce7044f85bb11d54f825b9fed904dac1b7c3f505c50cc8a43ab

42192e9df6321af2a1039a2353f1abe2aa53174582c7623cb1e42c9accc24720

11ddfdf2f102cb1518c0dc8d9021d8c16c9da3ae1b99ff3abc77467e7709ef23

dd5157b908d14f09cedc7ce687056a57a883fd796624e42f731c57630d7b43b4

34acd86d85b018feecc9adcd7985f15678306f518c21fcd6b34d62b27521fea5

4b3629ff14f5dc465d628cadc2f0c0b7503979078b1f9559fc35f6b0b1c7299d

7ecb85692b45c28300144c1451ef9e94cdd1964f40cd809e4b9b423581b2843e

9033aff8650ff5236b696561f7b0546581c74d715301a22584fdfca59ec444a2

68e376573d59d8f4e626d34df4ed8c16bae409fd95ca5f7215c9e483422ea429

8118b4c86db92483bf20e466f3ff664a4ea25e728a480282b498e95673bbb4f5

546a7635330fdefc2a084483eb2a43187d302de5bdfbe7a36364f8ed019f8f36

914cb1bcb371622923ac70bea30eb9bd6ff6f75c189d110de0be6adc30002157

28d9875c987188f940606459fd9b9dd65df224dfeb31e552e5b564a71b1eb7ce

ed2898dbbb1c9f3ba50adb64d17b1ce4ab31b3b0b8e18160ec6b6800f3922f9b

312ca68ff36542efe4f4b545230fc579269b477ec59f735081f395a5094c55c2

Picus Threat Library

809371 RedFlare (FireEye) Hacking Tool .EXE File Download Variant-3

207277 RedFlare (FireEye) Hacking Tool .EXE File Download Variant-2

867336 RedFlare (FireEye) Hacking Tool .EXE File Download Variant-1

3.14 RedFlare (GoRAT)

GoRAT is a RAT (Remote Access Trojan) written in the Golang programming language.

GoRAT IOCs (SHA256)

1381107c1f473b3dce170356158be445afc76ec3c0661d8429ef1f5a591e76f0
39845d02f72d83ef342b62b7348776d44cdb3eb6416b83ea2167b301d306cd58

3.15 ResumePlease

It is a Microsoft Office macro malware template that includes malicious VBA (Visual Basic for Application) codes.

ResumePlease IOCs (SHA256)

1866449e8ad2c55240eafdf14fc835138ca3e99a7b180c2150cef047868f56cc
a841a86fe10e11ced850a471cc3256e37d9435e292cac2a9c00f55592b2bf0de

Picus Threat Library
637798 ResumePlease (FireEye) Office Exploit Payload .Doc File Download Variant-1

3.16 SharPersist

It is a Windows persistence toolkit written in C# for FireEye Red Team [30]. It provides persistence via several methods, such as modifying registry run keys, adding payload to the startup folder, and adding a new scheduled task that runs on each startup.

MITRE ATT&CK Techniques
T1112 Modify Registry

T1546.015 Event Triggered Execution: Component Object Model Hijacking

T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

T1047 Windows Management Instrumentation

T1053.005 Scheduled Task/Job: Scheduled Task

SharPersist IOCs (SHA256)

e9711f47cf9171f79bf34b342279f6fd9275c8ae65f3eb2c6ebb0b8432ea14f8
455aab141cc9945899c9838b187251c7f647470d827a1d4ce8e833f04a6dd386
68c3388de07d92023490fb47caf1b6f92556959f2267cc3b3d2fcd5018cd3d72
0a443ea08c23991d229ee89a92bc23f959e17819027bb71f6267a7dfeeb9793d
4c3d4cbeec3d722929d86c0bf19108b3eac090fc5dc8fcde2cf818ff16e6fc5b

Picus Threat Library
206268 Registry Run Keys / Startup Folder Persistence by using SharPersist Tool

478660 SharpPersist (FireEye) Hacking Tool .EXE File Download Variant-3

286882 SharpPersist (FireEye) Hacking Tool .EXE File Download Variant-2

479515 SharpPersist (FireEye) Hacking Tool .EXE File Download Variant-1

3.17 SharPivot

SharPivot is a .NET console application. This red team tool executes commands on a remote target for lateral movement by utilizing DCOM (Distributed Component Object Model)

MITRE ATT&CK Techniques
T1021.003 Remote Services: Distributed Component Object Model

T1559.001 Inter-Process Communication: Component Object Model

T1059.003 Command and Scripting Interpreter: Windows Command Shell

3.18 SharpSchTask

It is a persistence tool written in C# that utilizes the scheduled task feature of Windows.

MITRE ATT&CK Techniques
Scheduled Task/Job: Scheduled Task

3.19 SharpStomp

SharpStomp is a C# utility that can be used to modify creation, last access, and last write time of a file. In other words, it is a timestomping tool.

MITRE ATT&CK Techniques
T1070.006 Indicator Removal on Host: Timestomp

3.20 SinfulOffice

This tool is used to create malicious Microsoft Office documents using the OLE (Object Linking and Embedding) feature.

SinfulOffice IOCs (SHA256)

4c5e5e172d233680fee184643b4b79dbf1f97674807c7e40bcfaac8675016c0d
a099840e55c6d813db791842efb1512e401af03e4fd9e285b6e906b615cc477a

Picus Threat Library
589557 OLE_CharENCODING (FireEye) Office Exploit Payload .DOC File Download Variant-1

3.21 WildChild

WildChild is a builder tool that is used to create malicious HTA (HTML Application) files. Microsoft HTML Application Host (Mshta.exe) runs HTA files.

MITRE ATT&CK Techniques
T1218.005 Signed Binary Proxy Execution: Mshta

3.22 WMIRunner

This tool is used to run WMI commands.

MITRE ATT&CK Techniques
T1047 Windows Management Instrumentation

3.23 WMISharp

This tool includes WMI commands used in Red Team engagements.

MITRE ATT&CK Techniques
T1047 Windows Management Instrumentation

3.24 WMISpy

WMISpy tool uses several WMI classes such as Win32_NetworkLoginProfile, MSFT_NetNeighbor, Win32_IP4RouteTable, Win32_DCOMApplication, Win32_SystemDriver, Win32_Share, and Win32_Process for reconnaissance and lateral movement.

MITRE ATT&CK Techniques
T1047 Windows Management Instrumentation

T1021.003 Remote Services: Distributed Component Object Model

4. **Tools without Adequate Data to Analyze**

The Yara rules published by FireEye for the following tools are specific to ProjectGuid of the tool. We hope FireEye publishes more detailed countermeasures about this tool.

4.1 AllTheThings
4.2 CoreHound
4.3 Justask
4.4 PrepShellCode
4.5 Revolver
4.6 SharpGenerator
4.7 SharpGrep
4.8 SharpSack
4.9 SharpSectionInjection
4.10 SharPy

References

[1] “LOLBAS.” [Online]. Available: https://lolbas-project.github.io. [Accessed: 09-Dec-2020]

[2] “APT29.” [Online]. Available: https://attack.mitre.org/groups/G0016/. [Accessed: 10-Dec-2020]

[3] E. Nakashima and J. Marks, “Spies with Russia’s foreign intelligence service believed to have hacked a top American cybersecurity firm and stolen its sensitive tools,” *The Washington Post*, The Washington Post, 08-Dec-2020 [Online]. Available: https://www.washingtonpost.com/national-security/leading-cybersecurity-firm-fireeye-hacked/2020/12/08/a3369aaa-3988-11eb-98c4-25dc9f4987e8_story.html. [Accessed: 10-Dec-2020]

[4] fireeye, “fireeye/red_team_tool_countermeasures.” [Online]. Available: https://github.com/fireeye/red_team_tool_countermeasures. [Accessed: 10-Dec-2020]

[5] “[No title].” [Online]. Available: https://raw.githubusercontent.com/fireeye/red_team_tool_countermeasures/master/rules/ADPASSHUNT/production/yara/APT_HackTool_MSIL_ADPassHunt_2.yar. [Accessed: 09-Dec-2020]

[6] Chris and V. my C. Profile, “GPP Password Retrieval with PowerShell.” [Online]. Available: http://obscuresecurity.blogspot.com/2012/05/gpp-password-retrieval-with-powershell.html. [Accessed: 09-Dec-2020]

[7] PowerShellMafia, “PowerShellMafia/PowerSploit.” [Online]. Available: https://github.com/PowerShellMafia/PowerSploit. [Accessed: 09-Dec-2020]

[8] “Beacon Covert C2 Payload - Cobalt Strike.” [Online]. Available: https://www.cobaltstrike.com/help-beacon. [Accessed: 09-Dec-2020]

[9] GhostPack, “GhostPack/Seatbelt.” [Online]. Available: https://github.com/GhostPack/Seatbelt. [Accessed: 09-Dec-2020]

[10] cobbr, “cobbr/SharpSploit.” [Online]. Available: https://github.com/cobbr/SharpSploit. [Accessed: 09-Dec-2020]

[11] med0x2e, “med0x2e/RT-EWS.” [Online]. Available: https://github.com/med0x2e/RT-EWS. [Accessed: 09-Dec-2020]

[12] GhostPack, “GhostPack/Rubeus.” [Online]. Available: https://github.com/GhostPack/Rubeus. [Accessed: 09-Dec-2020]

[13] “Steal or Forge Kerberos Tickets: Kerberoasting.” [Online]. Available: https://attack.mitre.org/techniques/T1558/003/. [Accessed: 09-Dec-2020]

[14] med0x2e, “med0x2e/GadgetToJScript.” [Online]. Available: https://github.com/med0x2e/GadgetToJScript. [Accessed: 09-Dec-2020]

[15] SecureAuthCorp, “SecureAuthCorp/impacket.” [Online]. Available: https://github.com/SecureAuthCorp/impacket. [Accessed: 09-Dec-2020]

[16] denandz, “denandz/KeeFarce.” [Online]. Available: https://github.com/denandz/KeeFarce. [Accessed: 09-Dec-2020]

[17] Kevin-Robertson, “Kevin-Robertson/InveighZero.” [Online]. Available: https://github.com/Kevin-Robertson/InveighZero. [Accessed: 09-Dec-2020]

[18] med0x2e, “med0x2e/NET-Assembly-Inject-Remote.” [Online]. Available: https://github.com/med0x2e/NET-Assembly-Inject-Remote. [Accessed: 09-Dec-2020]

[19] med0x2e, “med0x2e/NoAmci.” [Online]. Available: https://github.com/med0x2e/NoAmci. [Accessed: 09-Dec-2020]

[20] BloodHoundAD, “BloodHoundAD/SharpHound3.” [Online]. Available: https://github.com/BloodHoundAD/SharpHound3. [Accessed: 09-Dec-2020]

[21] BloodHoundAD, “BloodHoundAD/BloodHound.” [Online]. Available: https://github.com/BloodHoundAD/BloodHound. [Accessed: 09-Dec-2020]

[22] GhostPack, “GhostPack/SafetyKatz.” [Online]. Available: https://github.com/GhostPack/SafetyKatz. [Accessed: 09-Dec-2020]

[23] IllidanS, “IllidanS4/SharpUtils.” [Online]. Available: https://github.com/IllidanS4/SharpUtils. [Accessed: 09-Dec-2020]

[24] nccgroup, “nccgroup/nccfsas.” [Online]. Available: https://github.com/nccgroup/nccfsas. [Accessed: 09-Dec-2020]

[25] rasta-mouse, “rasta-mouse/RuralBishop.” [Online]. Available: https://github.com/rasta-mouse/RuralBishop. [Accessed: 09-Dec-2020]

[26] fireeye, “fireeye/DueDLLigence.” [Online]. Available: https://github.com/fireeye/DueDLLigence. [Accessed: 09-Dec-2020]

[27] ghogen, “MSBuild.” [Online]. Available: https://docs.microsoft.com/en-us/visualstudio/msbuild/msbuild. [Accessed: 09-Dec-2020]

[28] “Process Injection: Process Hollowing.” [Online]. Available: https://attack.mitre.org/techniques/T1055/012/. [Accessed: 09-Dec-2020]

[29] stevewhims, “mofcomp.” [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/wmisdk/mofcomp. [Accessed: 09-Dec-2020]

[30] fireeye, “fireeye/SharPersist.” [Online]. Available: https://github.com/fireeye/SharPersist. [Accessed: 09-Dec-2020]

[31] SolarWinds, SolarWinds Security Advisory, https://www.solarwinds.com/securityadvisory [Accessed: 14-Dec-2020]

[32] Reuters, Technology News, https://www.reuters.com/article/us-usa-solarwinds-cyber-idUSKBN28N0Y7 [Accessed: 14-Dec-2020]