Windows 10: protection, detection, and response against recent Depriz malware attacks

blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/

December 10, 2016

A few weeks ago, multiple organizations in the Middle East fell victim to targeted and destructive attacks that wiped data from computers, and in many cases rendering them unstable and unbootable. Destructive attacks like these have been observed repeatedly over the years and the Windows Defender and Windows Defender Advanced Threat Protection Threat Intelligence teams are working on protection, detection, and response to these threats.

Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as TERBIUM, following our internal practice of assigning rogue actors chemical element names.

Although the extent of damage caused by this latest attack by TERBIUM is still unknown, Windows 10 customers have a set of features available for them to enable to mitigate such attack. Windows 10 has built-in proactive security components, such as Device Guard, that mitigate this threat; Windows Defender customers are protected through multiple signature-based detections; and Windows Defender Advanced Threat Protection (ATP) customers are provided extensive visibility and detection capabilities across the attack kill chain, enabling security operation teams to respond quickly. Microsoft's analysis has shown that the components and techniques used by TERBIUM in this campaign trigger multiple detections and threat intelligence alerts in Windows Defender Advanced Threat Protection.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

Attack composition

Microsoft Threat Intelligence has observed that the malware used by TERBIUM, dubbed "Depriz" by Microsoft, reuses several components and techniques seen in the 2012 attacks, and has been highly customized for each targeted organization.

We do not see any indicators that a zero-day exploit is being used by TERBIUM.

Step 1: Writing to disk

The initial infection vector TERBIUM uses is unknown. As credentials have been hard-coded in the malware TERBIUM uses, it is suspected that TERBIUM has harvested credentials or infiltrated the target organization previously. Once TERBIUM has a foothold in the organization, its infection chain starts by writing an executable file to disk that contains all the components required to carry out the data-wiping operation. These components are encoded in the executables resources as fake bitmap images.

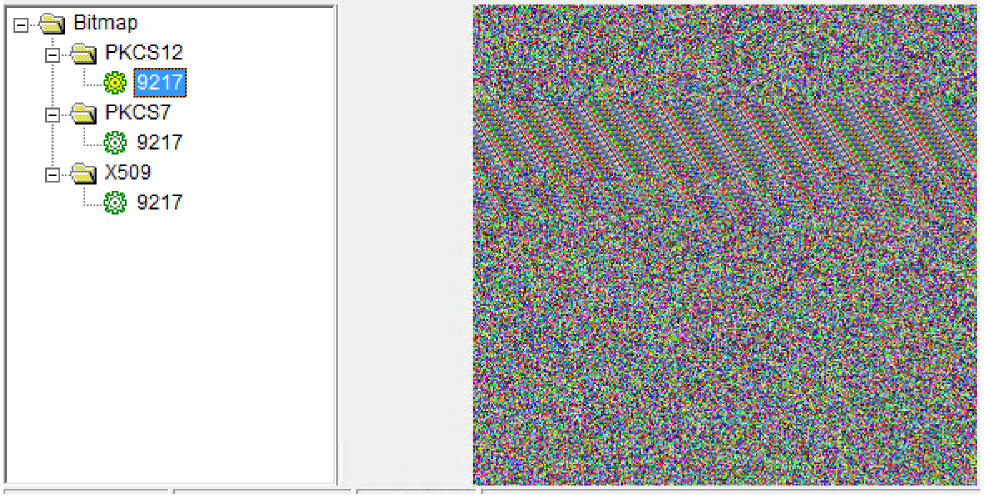


Figure 1. The components of the Trojan are fake bitmap images

We decoded the components as the following files:

- PKCS12 – a destructive disk wiper component
- PKCS7 – a communication module
- X509 – 64-bit variant of the Trojan/implant

Step 2: Propagation and persistence through the target network

We have seen TERBIUM use hardcoded credentials embedded in the malware to propagate within a local network. The availability of these credentials to the activity group suggests that the attacks are highly targeted at specific enterprises.

The propagation and persistence is carried out as follows:

1. First, it tries to start the *RemoteRegistry* service on the computer it is trying to copy itself to, then uses *RegConnectRegistryW* to connect to it.
2. Next, it attempts to disable UAC remote restrictions by setting the *LocalAccountTokenFilterPolicy* registry key value to *"1"*.
3. Once this is done, it connects to the target computer and copies itself as *%System%\ntssrvr32.exe* or *%System%\ntssrvr64.exe* before setting either a remote service called "*ntssv*" or a scheduled task.

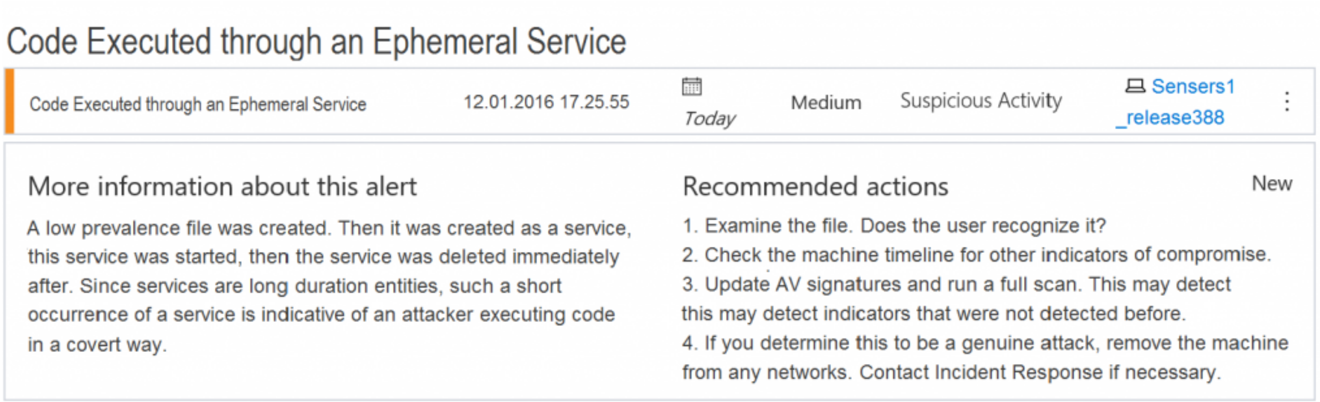
Step 3: Wiping the machine

Next, the Trojan installs the wiper component. Note: TERBIUM establishes a foothold throughout the organization and does not proceed with the destructive wiping operation until a specific date/time: November 17, 2016 at 8:45 p.m.

The wiper component is installed as *%System%\<random name>.exe.* During our testing, it used the name "*routeman.exe*", but static analysis shows it can use several other names that attempt to imitate file names of legitimate system tools.

The wiper component also contains encoded files in its resources as fake bitmap images.

The first encoded resource is a legitimate driver called *RawDisk* from the Eldos Corporation that allows a user mode component raw disk access. The driver is saved as *%System%\drivers\drdisk.sys* and installed by creating a service pointing to it using "*sc create*" and "*sc start*". This behavior can be observed in the process tree available in the Windows Defender ATP portal. The below alert represents an example of the generic detections in Windows Defender ATP:



Code Executed through an Ephemeral Service

Code Executed through an Ephemeral Service | 12.01.2016 17.25.55 | Today | Medium | Suspicious Activity | Sensers1 _release388

More information about this alert

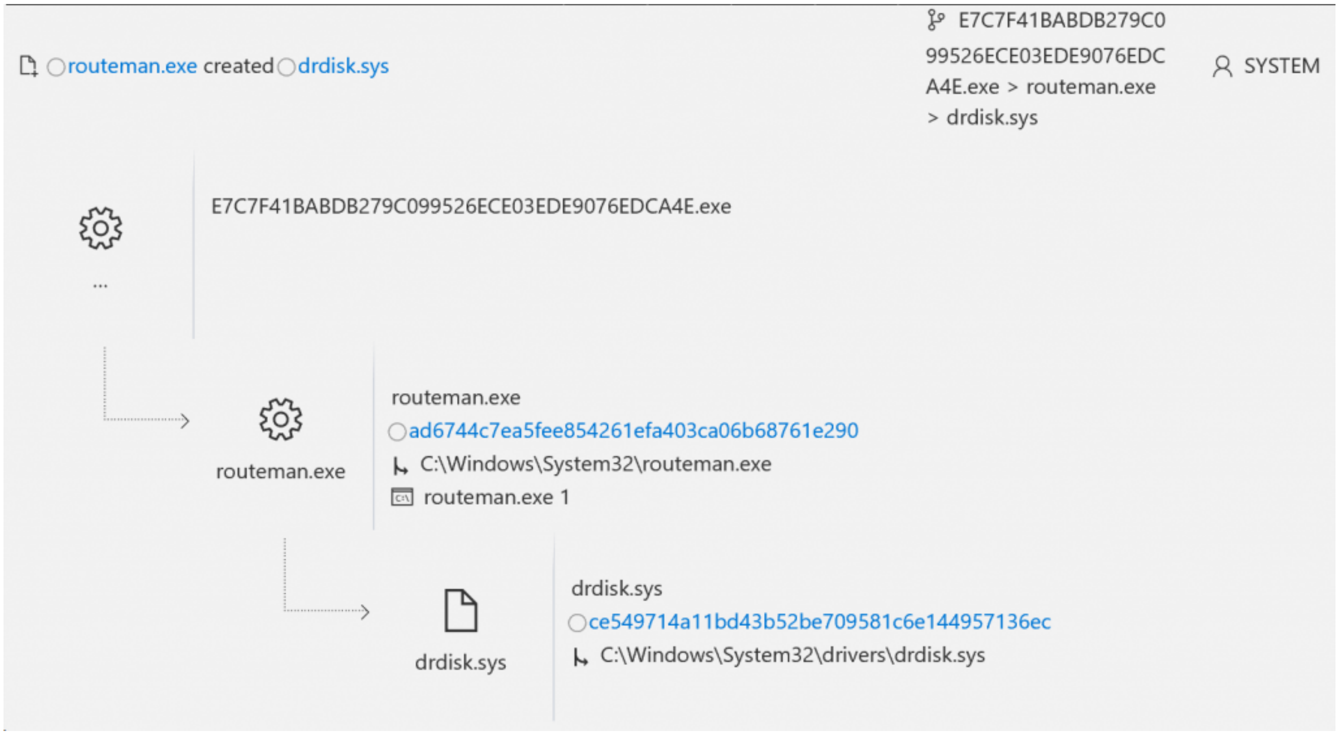
A low prevalence file was created. Then it was created as a service, this service was started, then the service was deleted immediately after. Since services are long duration entities, such a short occurrence of a service is indicative of an attacker executing code in a covert way.

Recommended actions

New

1. Examine the file. Does the user recognize it?
2. Check the machine timeline for other indicators of compromise.
3. Update AV signatures and run a full scan. This may detect this may detect indicators that were not detected before.
4. If you determine this to be a genuine attack, remove the machine from any networks. Contact Incident Response if necessary.

Figure 2. Windows Defender ATP alert: Depriz starting ephemeral service to load RawDisk driver "drdisk"



○routeman.exe created○drdisk.sys

E7C7F41BABDB279C099526ECE03EDE9076EDCA4E.exe > routeman.exe > drdisk.sys

SYSTEM

E7C7F41BABDB279C099526ECE03EDE9076EDCA4E.exe

routeman.exe

routeman.exe
○ad6744c7ea5fee854261efa403ca06b68761e290
C:\Windows\System32\routeman.exe
routeman.exe 1

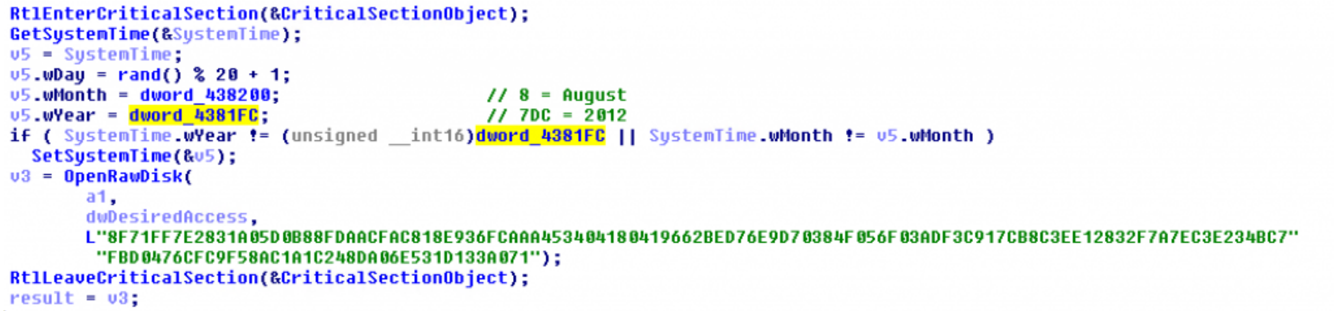
drdisk.sys

drdisk.sys
○ce549714a11bd43b52be709581c6e144957136ec
C:\Windows\System32\drivers\drdisk.sys

Figure 3. Windows Defender ATP event tree: Depriz Trojan dropping the wiper component (named "routeman" in this instance), which in turn drops the RawDisk driver "drdisk"

There are two interesting things worth noting about *RawDisk*:

- It requires a valid license key from Eldos Corporation to run. However, the license key included in Depriz is the same as the one used in the 2012 attacks – and this license key was only valid for a short period in 2012. TERBIUM works around this by changing the system time on targeted computers to a valid period in 2012.
- It is the same as the driver used in the 2012 attacks.



```
RtlEnterCriticalSection(&CriticalSectionObject);
GetSystemTime(&SystemTime);
v5 = SystemTime;
v5.wDay = rand() % 20 + 1;
v5.wMonth = dword_438200;                    // 8 = August
v5.wYear = dword_4381FC;                     // 7DC = 2012
if ( SystemTime.wYear != (unsigned __int16)dword_4381FC || SystemTime.wMonth != v5.wMonth )
  SetSystemTime(&v5);
v3 = OpenRawDisk(
       a1,
       dwDesiredAccess,
       L"8F71FF7E2831A05D0B88FDAACFAC818E936FCAAA45340418041966 2BED76E9D70384F056F03ADF3C917CB8C3EE12832F7A7EC3E234BC7"
        "FBD0476CFC9F58AC1A1C248DA06E531D133A071");
RtlLeaveCriticalSection(&CriticalSectionObject);
result = v3;
```

Figure 4. Depriz license key (the same as the one used in 2012 attacks) and its limited validity period

The wiper component uses an image file to overwrite files in locations listed in the following:

- *Master Boot Records (MBR)*
- *HKLM\System\CurrentControlSet\Control\SystemBootDevice*
- *HKLM\System\CurrentControlSet\Control\FirmwareBootDevice*
- *C:\Windows\System32\Drivers*
- *C:\Windows\System32\Config\systemprofile*
- Typical user folders like “*Desktop*”, “*Downloads*”, “*Documents*”, “*Pictures*”, “*Videos*” and “*Music*”

Microsoft is also aware of a second threat that uses a distinct wiping component. We detect this as Trojan:Win32/Cadlotcorg.A!dha in Defender and generic detections with Defender ATP. Microsoft is continuing to monitor for additional information on this threat.

Step 4: Rendering the machine unusable

Finally, the following command is used to reboot the system into the intended unusable state:

shutdown -r -f -t 2

When the computer attempts to restart after shutting down, it is unable to find the operating system because the MBR was overwritten in step 3. The machine will no longer boot properly.

Mitigation: Multiple layers of protection from Microsoft

Windows 10 protects, detects and responds to this threat. Windows 10 has built-in proactive security components, such as Device Guard, that mitigate this threat by restricting execution to trusted applications and kernel drivers.

In addition, Windows Defender detects and remediates all components on endpoints as Trojan:Win32/Depriz.A!dha, Trojan:Win32/Depriz.B!dha, Trojan:Win32/Depriz.C!dha, and Trojan:Win32/Depriz.D!dha.

Windows Defender Advanced Threat Protection (ATP), our post-breach security service, provides an additional layer of security to enterprise users. With threat intelligence indicators, generic detections, and machine learning models, Windows Defender ATP (trial link) provides extensive visibility and detection capabilities across the attack kill chain of threats like TERBIUM.

Appendix – Indicators of compromise

We discovered the following SHA1s in relation to TERBIUM:

SHA1 hashes for malicious files

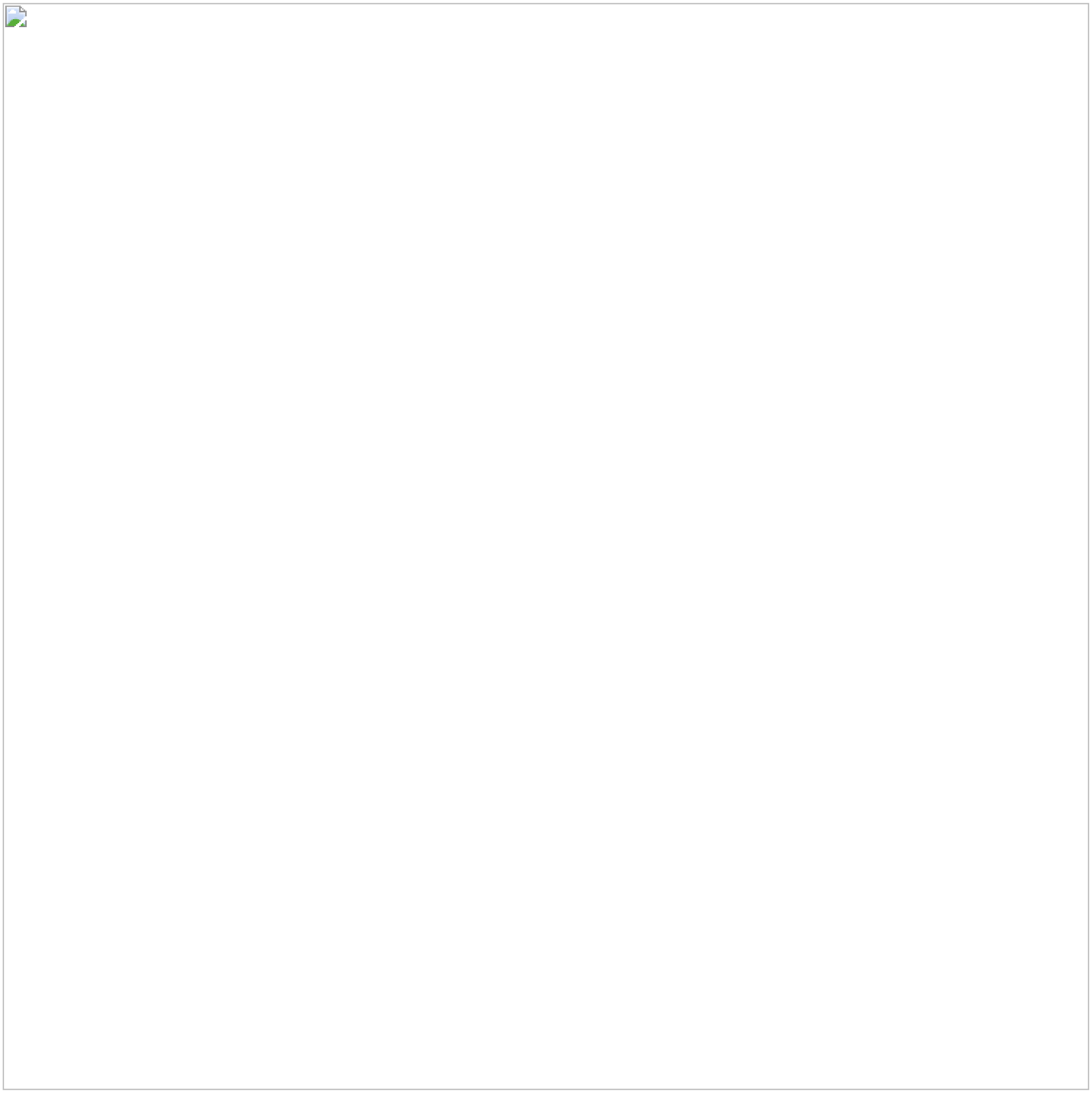
- 5c52253b0a2741c4c2e3f1f9a2f82114a254c8d6
- e7c7f41babdb279c099526ece03ede9076edca4e
- a2669df6f7615d317f610f731b6a2129fbed4203
- 425f02028dcc4e89a07d2892fef9346dac6c140a
- ad6744c7ea5fee854261efa403ca06b68761e290

SHA1 hashes for legitimate RawDisk drivers

- 1292c7dd60214d96a71e7705e519006b9de7968f
- ce549714a11bd43b52be709581c6e144957136ec

Signature names for malicious files

Mathieu Letourneau



Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.