Ransomware: groeiend aantal aanvallers dat virtuele machines gebruikt

Tactic verbergt de lading van ransomware en verlaagt het risico op ontdekking terwijl het versleutelingsproces aan de gang is.

Symantec heeft bewijs gevonden dat een toenemend aantal ransomware-aanvallers virtuele machines (VM's) gebruikt om hun ransomware-payloads uit te voeren op gecompromitteerde computers. De motivatie achter de tactiek is stealth. Om argwaan te wekken of antivirussoftware te activeren, zal de ransomware-payload zich "verbergen" in een VM terwijl de bestanden op de hostcomputer worden versleuteld.

De tactiek is een recente ontwikkeling, die vorig jaar door Sophos is gedocumenteerd in verband met RagnarLocker. In dat geval werd ransomware uitgevoerd vanuit een Oracle VirtualBox Windows XP VM.

VirtualBox-gebruik

Tijdens een recent onderzoek naar een poging tot ransomware-aanval ontdekte Symantec dat de aanvallers een VirtualBox VM hadden geïnstalleerd op sommige gecompromitteerde computers. In tegenstelling tot de eerder gedocumenteerde RagnarLocker-aanvallen, waarbij Windows XP betrokken was, leek de VM in dit geval Windows 7 te draaien.

De VM is aan het doel geleverd via een kwaadaardig installatiebestand dat verschillende bestandsnamen gebruikte, waaronder:

- fuckyou.msi
- fuck.msi
- aa51978f.msi
- s3c.msi

Het installatieprogramma heeft een bestand gemaakt met de naam runner.exe, een uitvoerbaar bestand van Golang (Go), gecompileerd uit het volgende bronbestand:

- C:/builder/runner/main.go

Afgezien van standaard Go-bibliotheken, gebruikte het de go-ps-bibliotheek voor procesopsomming. Ingesloten tekenreeksen die door het uitvoerbare bestand werden gebruikt, zoals bestandsnamen, procesnamen en opdrachten, werden verdoezeld met behulp van vier-byte XOR-sleutels. Elke string is versleuteld met een unieke sleutel.

Dit uitvoerbare bestand was afhankelijk van meerdere andere bestanden die naar verwachting in dezelfde map aanwezig zouden zijn. Het belangrijkste doel was om een VirtualBox VM te installeren in een headless-modus.

Bij uitvoering heeft runner.exe de volgende acties uitgevoerd:

- Het controleerde of het op de Active Directory (AD)-controller draaide op basis van de aanwezigheid van de *C:\Windows\SYSVOL-* directory. Het werd afgesloten als de controle waar bleek te zijn.
- Het gebruikte een functie genaamd russianDetect om te controleren of het draaide op een systeem met een Russische toetsenbordindeling (0x0419). Het werd afgesloten als de cheque waar bleek te zijn. Dergelijke controles zijn een veelvoorkomend kenmerk van gerichte ransomware-aanvallen.
- Het somde lopende processen en services op en beëindigde alle processen die aanwezig waren op zwarte lijsten (procBlacklist, servicesBlacklist) met behulp van *taskkill.exe* en *sc.exe.*

Het uitvoerbare bestand liet vervolgens een bestand met de naam starter.bat vallen, voerde het uit en verwijderde het met de volgende inhoud om een herstelpartitie aan te koppelen:

- *mountvol E:\ \\?\Volume{<ID>}*

Vervolgens decodeerde en dropte het VirtualBox.xml, een VirtualBox-configuratiebestand, en micro.xml, een VM-configuratiebestand (zie appendix). Het creëerde een SDRSMLINK-directory en koppelde systeembestanden aan die directory, bijvoorbeeld:

- *cmd /C mklink /j "%SYSTEMROOT%\SDRSMLINK\Program Files" "%SYSTEMROOT%\Program Files"*

Het heeft ook de sectie "<SharedFolders>" in micro.xml aangepast om de bestanden en mappen weer te geven die zijn gekoppeld in

CSIDL_WINDOWS\SDRSMLINK. Vervolgens initialiseerde het VirtualBox-componenten:

```
cmd /C sc create VBoxDRV binpath= %SYSTEMROOT%\\app64\drivers\VBoxDrv.sys
type= kernel start= auto error= normal displayname= PortableVBoxDRV
regsvr32 /S %SYSTEMROOT%\\app64\VBoxC.dll
cmd /C %SYSTEMROOT%\\app64\VBoxSVC.exe /reregserver
rundll32 %SYSTEMROOT%\\app64\VBoxRT.dll ,RTR3Init
```

Het inventariseerde en wist Windows-systeemlogboeken met behulp van WEvtUtil.exe:

```
wevtutil.exe enum-logs
wevtutil.exe clear-log <LOG_NAME>
```

Symantec kreeg geen VM-image, maar wat waarschijnlijk daarna gebeurde, was dat de ransomware-payload zich op de schijf van de VM bevond en automatisch startte zodra het besturingssysteem volledig was opgestart. De VM had waarschijnlijk toegang tot de bestanden en mappen van de hostcomputer (via "SharedFolders" ingesteld door runner.exe), waardoor het bestanden op de hostcomputer kon versleutelen.

Conti of Mount Locker?

Hoewel de payload die in de VM draaide niet werd geïdentificeerd, waren er redelijk sterke aanwijzingen dat het Conti was. Een combinatie van gebruikersnaam en wachtwoord (nuuser/7HeC00l3stP@ssw0rd) die bij deze aanvallen werd gebruikt, werd eerder in verband gebracht met oudere Conti-activiteit, daterend uit april 2021.

Op dezelfde computer waarop de VM was geïmplementeerd, zag Symantec echter ook dat Mount Locker werd ingezet, wat de vraag opriep of de payload daadwerkelijk Mount Locker was. Aangezien het belangrijkste doel van het uitvoeren van een payload op een VM is om detectie te voorkomen, heeft het weinig zin voor de aanvaller om de payload ook op de hostcomputer te implementeren.

Een mogelijke verklaring is dat de aanvaller een aangesloten operator is met toegang tot zowel Conti als Mount Locker. Ze hebben mogelijk geprobeerd een payload (Conti of Mount Locker) op een virtuele machine uit te voeren en, toen dat niet werkte, hebben ze ervoor gekozen om Mount Locker op de hostcomputer uit te voeren.

Kwaadaardige activiteit verdoezelen

Ransomware-operators verfijnen voortdurend hun tactieken om detectie een stap voor te blijven. Velen vertrouwen nu sterk op legitieme tools en tools voor tweeërlei gebruik om aanvallen op gerichte netwerken uit te voeren. De

ransomware-payload zelf is vaak het stadium van de aanval dat de meeste kans heeft om rode vlaggen te veroorzaken en door het te verbergen in een virtuele machine, is er een verwachting dat het misschien niet wordt ontdekt. Organisaties moeten extra waakzaam zijn met betrekking tot de ongeoorloofde installatie van virtuele machines op hun netwerken.

Bescherming/mitigatie

Ga voor de nieuwste beveiligingsupdates naar het Symantec Protection Bulletin .

Indicatoren van compromis

- 2eae8e1c2e59527b8b4bb454a51b65f0ea1b0b7476e1c80b385f579328752836 - Installateur
- 9f801a8d6b4801b8f120be9e5a157b0d1fc3bbf6ba11a7d202a9060e60b707d8 - runner.exe
- e5291bae18b0fa3239503ab676cacb12f58a69eb2ec1fd3d0c0702b5a29246cb - VirtualBox
- d89bd47fb457908e8d65f705f091372251bae3603f5ff59afb2436abfcf976d8 - Mountlocker
- 8f247e4149742532b8a0258afd31466f968af7b5ac01fdb7960ac8c0643d2499 - Mountlocker

Bijlage

VirtualBox.xml - VirtualBox-configuratiebestand

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Sun VirtualBox Global Configuration -->
<VirtualBox xmlns="http://www.innotek.de/VirtualBox-settings" version="1.7-windows">
  <Global>
    <ExtraData>
      <ExtraDataItem name="GUI/UpdateDate" value="1 d, 2020-05-05"/>
      <ExtraDataItem name="GUI/SUNOnlineData" value="triesLeft=2"/>
      <ExtraDataItem name="GUI/LastWindowPostion" value="298,109,770,550"/>
    </ExtraData>
    <MachineRegistry>
      <MachineEntry uuid="{ea68756b-4a61-4f99-a824-82bd26041256}" src="micro.xml"/>
    </MachineRegistry>
    <MediaRegistry>
      <HardDisks>
        <HardDisk uuid="{a9605e9f-31df-4dc6-827c-5b684f32bb64}" location="micro.vdi" format="VDI" type="Normal"/>
      </HardDisks>
      <DVDImages/>
      <FloppyImages/>
    </MediaRegistry>
    <NetserviceRegistry>
```

```
      <DHCPServers>
        <DHCPServer networkName="HostInterfaceNetworking-VirtualBox Host-
Only Ethernet Adapter" IPAddress="192.168.56.100"
networkMask="255.255.255.0" lowerIP="192.168.56.101"
upperIP="192.168.56.254" enabled="1"/>
      </DHCPServers>
    </NetserviceRegistry>
    <USBDeviceFilters/>
    <SystemProperties defaultMachineFolder="." defaultHardDiskFolder="."
defaultHardDiskFormat="VDI" remoteDisplayAuthLibrary="VRDPAuth"
webServiceAuthLibrary="VRDPAuth" LogHistoryCount="3"/>
  </Global>
</VirtualBox>
```

Micro.xml - configuratiebestand voor virtuele machines

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Sun VirtualBox Machine Configuration -->
<VirtualBox xmlns="http://www.innotek.de/VirtualBox-settings" version="1.7-
windows">
  <Machine uuid="{ea68756b-4a61-4f99-a824-82bd26041256}" name="micro"
OSType="Windows7" lastStateChange="2020-05-13T03:49:05Z">
    <ExtraData>
      <ExtraDataItem name="GUI/SaveMountedAtRuntime" value="yes"/>
      <ExtraDataItem name="GUI/ShowMiniToolBar" value="yes"/>
      <ExtraDataItem name="GUI/MiniToolBarAlignment" value="bottom"/>
      <ExtraDataItem name="GUI/LastWindowPostion" value="8,31,800,643"/>
      <ExtraDataItem name="GUI/Fullscreen" value="off"/>
      <ExtraDataItem name="GUI/Seamless" value="off"/>
      <ExtraDataItem name="GUI/AutoresizeGuest" value="on"/>
      <ExtraDataItem name="GUI/MiniToolBarAutoHide" value="on"/>
    </ExtraData>
    <Hardware>
      <CPU count="1">
        <HardwareVirtEx enabled="true"/>
        <PAE enabled="true"/>
      </CPU>
      <Memory RAMSize="512"/>
      <Boot>
        <Order position="3" device="HardDisk"/>
      </Boot>
      <Display VRAMSize="12" monitorCount="1" accelerate3D="false"/>
      <RemoteDisplay enabled="false" port="43399" authType="Null"/>
      <BIOS>
        <ACPI enabled="true"/>
        <IOAPIC enabled="false"/>
        <Logo fadeIn="true" fadeOut="true" displayTime="0"/>
        <BootMenu mode="MessageAndMenu"/>
        <TimeOffset value="0"/>
        <PXEDebug enabled="false"/>
      </BIOS>
      <DVDDrive passthrough="false"/>
      <FloppyDrive enabled="false"/>
      <USBController enabled="false" enabledEhci="false"/>
      <Network/>
      <UART>
        <Port slot="0" enabled="false" IOBase="0x3f8" IRQ="4"
hostMode="Disconnected"/>
        <Port slot="1" enabled="false" IOBase="0x3f8" IRQ="4"
hostMode="Disconnected"/>
      </UART>
      <LPT>
        <Port slot="0" enabled="false" IOBase="0x378" IRQ="4"/>
```

```
        <Port slot="1" enabled="false" IOBase="0x378" IRQ="4"/>
      </LPT>
      <AudioAdapter controller="AC97" driver="DirectSound"
enabled="false"/>
      <SharedFolders/>
      <Clipboard mode="Bidirectional"/>
      <Guest memoryBalloonSize="0" statisticsUpdateInterval="0"/>
      <GuestProperties>
        <GuestProperty name="/VirtualBox/HostInfo/GUI/LanguageID" value="C"
timestamp="1589341300166459600" flags=""/>
      </GuestProperties>
    </Hardware>
    <StorageControllers>
      <StorageController name="IDE" type="PIIX4" PortCount="2">
        <AttachedDevice type="HardDisk" port="0" device="0">
          <Image uuid="{a9605e9f-31df-4dc6-827c-5b684f32bb64}"/>
        </AttachedDevice>
      </StorageController>
    </StorageControllers>
  </Machine>
</VirtualBox>
```

Over de auteur

Threat Hunter-team

Symantec

Het Threat Hunter-team is een groep beveiligingsexperts binnen Symantec met als missie het onderzoeken van gerichte aanvallen, het stimuleren van verbeterde bescherming in Symantec-producten en het bieden van analyses waarmee klanten op aanvallen kunnen reageren.