??????? ?????? - ?????? ???? ?????? ??????

??? ????????

بياناتٌ تدريبيةٌ - برمجيةٌ فديةٌ موقّعةٌ رقميًا (Hive)

?????????

في هذا السيناريو التدريبي، سننفذ حمولة برمجية فدية، تعمل بصلاحيات المسؤول (admin)، وموقّعة بتوقيع مخصص. ال يختلف هذا السيناريو كثيرًا عن العينة "**الأساسية**"، لكنه يستخدم ملفًا تنفيذيًا موقّعًا.

غالبًا ما تُعامل الملفات التنفيذية الموقّعة على أنها موثوقة تلقائيًا. صحيح أن البرمجيات المعتمدة □□□ أن تكون كلها موقّعة، لكن هذه ليست عالقة ثنائية الاتجاه، والا ينبغي لنا الوثوق بالأشياء □□□□ أنها موقّعة. للأسف، يُرتكب هذا الخطأ في بعض الأحيان.

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

بصرف النظر عن أن اسم هذه الشهادة غريب بعض الشيء لأغراض التدريب، كيف يعرف Cyber Crucible أنها غير موثوقة؟ يتوخى Cyber Crucible الحذر ويحتفظ بقائمة (خاصة بكل مجموعة) من الشهادات الموثوقة. وهذا يعني أنه يمكننا بسهولة اكتشاف شهادات التوقيع الاختبارية، بالإضافة إلى الشهادات الرسمية من جهات إصدار الشهادات (CAs) الكبرى مثل digicerts.

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

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 1:51:54 PM EDT	Worm Geum Indigo 180	False	False	True

يمكننا أن نرى أعلاه أنه على الرغم من أن الملف "321d0..." موقّع، إلا أنه لا يزال غير موثوق. وبما أنه لا توجد تقنيات تعتيم معقدة أخرى استُخدمت لنشر الهجوم، فإننا نعرف بالضبط من أين جاء!

للتأكد من 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 (child processes) مثيرة للاهتمام رغم ذلك. فحتى مع كون طريقة تنفيذ البرمجية الخبيثة نفسها واضحة، تُشغّل العديد من العمليات في الخلفية التي تعطّل 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، يكون الهجوم قد احتُوي بواسطة Cyber Crucible، لكن تحليل العمليات ذات الصلة مهم لتحديد نطاق السلوكيات الخبيثة. قد يبدو تنفيذ الملف التنفيذي غير الموقّع وحده واضحًا عندما يعرضه Cyber Crucible بهذا الشكل، لكن في كثير من الأحيان يتم تجاهل العمليات التي تُشغّل في الخلفية من قبل شيء محمي وذي صلاحيات مثل Defender ببساطة.

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

- Mitre T1566 - يمكن استخدام التصيّد الاحتيالي (Phishing) لخداع المستخدم لأداء إجراء ما كان ليقوم به لولا ذلك، مثل تشغيل نص برمجي أو مشاركة كلمة مرور.
- Mitre T1091 - قد تنسخ البرمجية الخبيثة نفسها على وسائط قابلة للإزالة بحيث يمكن للجهاز التالي الذي يتصل بها تنفيذها عبر التشغيل التلقائي (autorun) أو ثغرات برامج التشغيل (driver).
- Mitre T1204 - تنفيذ المستخدم، الذي غالبًا ما يتم الحصول عليه عبر التصيّد الاحتيالي، هو أبسط طريقة تبدأ بها البرمجيات الخبيثة تنفيذها.
- Mitre T1587-002 - شهادات توقيع الشيفرة البرمجية هي وسيلة لجهة معينة للتصديق على شيفرة أحد التطبيقات. قد تُنشئ البرمجيات الخبيثة شهادة ال تصدر عن أي جهة إصدار شهادات (certificate authority) لكنها قد تُربك المستخدم فيظن أنها شرعية.
- Mitre T1587-003 - تُستخدم شهادات SSL لضمان أن نقل البيانات موثوق. في بيئة سيئة الإعداد، قد تتمكن البرمجية الخبيثة من تثبيت شهادة SSL خاصة بها لتسهيل هجمات الوسيط (man in the middle).

Revision #1
Created 2026-07-24 02:22:08 UTC by Dennis Underwood
Updated 2026-07-24 02:22:08 UTC by Dennis Underwood