Bayerisches Landesamt
für Verfassungsschutz

Bayerisches Landesamt für Verfassungsschutz ·
Postfach 45 01 45 · 80901 München

Ihre Zeichen, Ihre Nachricht vom	Unser Zeichen		München
	337-S-050003.1/57/15		25.02.2022

Bearbeiter/in	Telefon	Telefax	E-Mail
	089 31201-222	089 31201-380	caz@lfv.bayern.de

Warnmeldung vor Wiper-Malware

Sehr geehrte Damen und Herren,

nach öffentlichen Berichten kommt es seit Mittwoch, dem 23.02.2022 zu erneuten Cyberangriffen mit einer bisher unbekannten Master-Boot-Record **Wiper-Malware** (NEARMISS, HermeticWiper, KillDisk.NCV und DriveSlayer). Diese Malware soll gegen mehrere hundert Computersysteme innerhalb der Ukraine eingesetzt worden sein, darunter Regierungsstellen, Militärdienstleister und Finanzinstitute. In zwei Fällen wurden Unternehmen im europäischen Ausland Opfer des Angriffs, bei denen es sich um Vertragspartner der ukrainischen Regierung handeln soll.

Trotz des bisherigen Fokus auf ukrainische Ziele besteht die reelle Gefahr, dass derartige Instrumente **auch gegen Ziele in Deutschland** eingesetzt werden, insbesondere gegen Firmen mit Geschäftsbeziehungen in die Ukraine.

Mehrere Samples der Malware sind auf der Plattform VirusTotal verfügbar und werden derzeit durch den Verfassungsschutzverbund analysiert. Weiterhin existieren bereits mehrere Analyseberichte von IT-Sicherheitsunternehmen.

Bei den aktuellen Angriffen wird keine angebliche Lösegeld-Forderung angezeigt, weiterhin ist die Malware durch die Firma "Hermetica Digital" digital signiert.

Telefon: 089 31201-222
Telefax: 089 31201-380
E-Mail: caz@lfv.bayern.de
Internet: www.lfv.bayern.de
Knorrstraße 139 · 80937 München
U2 (Frankfurter Ring)

Die Malware wurde außerdem mithilfe der Windows Gruppenrichtlinien (Group Policy Object) ausgebracht, was auf einen bereits vorher bestehenden Zugang der Angreifer zu den betroffenen Netzwerken hindeutet.

Gleichzeitig wurde der Angriff mit DDoS-Attacken und Web-Defacements flankiert.

Im Folgenden erhalten Sie deswegen erste Detektionsregeln und Hinweise. Zusätzlich weisen wir wegen des hohen Verbreitungsgrades daraufhin, dass die Firma Microsoft bereits Signaturen für den Antivirenscanner Windows Defender in Windows 10/11 entwickelt hat.

Detektionen der eingesetzten Malware würden demnach von Windows Defender unter folgenden Namen erkannt.

- DoS:Win32/ FoxBlade.A!dha
- DoS:Win32/ FoxBlade.A!dha
- TrojanDownloader:Win32/ PandoraBlade.A!dha
- Trojan:Win64/ PandoraBlade.B!dha

Bitte beachten Sie die **separat zum Download angebotenen** Indicators of Compromise (IoC) und YARA-Regel, zur Suche nach dem bereits ausgebrachten NEARMISS auf den eigenen Systemen. Den Link haben wir in der E-Mail übermittelt. Das Passwort dient lediglich dem Schutz vor Crawlern.

Ergänzende Informationen zu den IoC stellen wir nachfolgend dar:

HermeticWiper	SHA1
Win32 EXE	912342f1c840a42f6b74132f8a7c4ffe7d40fb77
Win32 EXE	61b25d11392172e587d8da3045812a66c3385451

Die Hashwerte der ausgebrachten Treiber (ms-compressed) sind in der folgenden Auflistung dargestellt. Da die EaseUS-Treiber legitim sind, könnten sie False Positives generieren. Sie können aber dennoch dazu dienen, einen Hinweis auf eine mögliche Kompromittierung zu geben.

ms-compressed	MD5
RCDATA_DRV_X64	a952e288a1ead66490b3275a807f52e5
RCDATA_DRV_X86	231b3385ac17e41c5bb1b1fcb59599c4

RCDATA_DRV_XP_X64	095a1678021b034903c85dd5acb447ad
RCDATA_DRV_XP_X86	eb845b7a16ed82bd248e395d9852f467

Darüber hinaus sind folgende **Handlungsempfehlungen** zu beachten:

Allgemeine Informationen

- Die Malware wird unter den Namen HermeticWiper, DriveSlayer und KillDisk.NCV geführt.
- Die Malware wurde mit einem gültigen Zertifikat signiert, das bisher bei keiner legitimen Datei entdeckt werden konnte.
    - Zertifikatsseriennummer:

      `0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC`

    - SHA256:

      `1ae7556dfacd47d9efbe79be974661a5a6d6d923`
- Malware nur etwa 114 KB groß
- Um Zugriff auf erweiterte Rechte zu erhalten verwendet die Malware einen legitimen Treiber für Partitionsmanagement EaseUS: „empntdrv.sys“.
- Die Malware verändert Registrywerte:
    - Der folgende Schlüssel wird auf den Wert: 0 gesetzt und so Crash dumps deaktiviert:

`SYSTEM\CurrentControlSet\Control\CrashControl CrashDumpEnabled`

    - Eine Veränderung dieses Wertes ist ein guter Indikator dafür, dass die Malware bereits auf dem entsprechenden System läuft
- Die Malware kann zu einem sprunghaften Anstieg der Nutzung des Memorys führen (beispielsweise durch den svchost.exe Prozess)

Handlungsempfehlungen für gefährdete Unternehmen

Da die Malware nur eine kurze Zeit benötigt, um ein System zu zerstören, ist Prävention in diesem Fall besonders wichtig.

- Weil der Angreifer für das Platzieren und die Ausführung der Malware eine Zugriffsmöglichkeit auf das System besitzen muss, ist es empfehlenswert mögliche Angriffsvektoren zu minimieren und sorgfältig zu überlegen, wel-

che Vorgänge und Systeme aktuell für die Gewährleistung der Funktionalitäten eines Unternehmens unbedingt erforderlich sind.

- Backups sollten in regelmäßigen Abständen angefertigt und anschließend von den betroffenen Systemen getrennt aufbewahrt werden.
- Updates: Bekannte Sicherheitslücken können durch das Einspielen vorhandener Patches geschlossen werden und so nicht als Angriffsvektor genutzt werden.
- Yara-Rules können nur detektieren, sie verhindern nicht die Ausführung. Eine Detektion erlaubt es aber schnell zu reagieren.
- Intrusion Detection Management Systeme (IDMS) sollten in der Lage sein die Malware zu erkennen und zu blockieren. Dafür muss dem IDMS die Berechtigung gegeben werden das Starten und Ausführen entsprechender Prozesse nicht nur zu protokollieren, sondern diese auch sofort stoppen und Dateien in Quarantäne verschieben zu können.
- Berechtigungen und Nutzer auf Systemen überprüfen: unbekannte oder nicht mehr verwendete Nutzer entfernen und Berechtigungen für Nutzer auf ein Minimum reduzieren

Offene Informationen sind unter anderem in folgenden Quellen zu finden:

- https://channel969.com/new-wiper-malware-concentrating-on-ukraine-amid-russias-army-operation/
- https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

Bitte melden Sie Trefferlagen zeitnah an uns zurück.

Wir stehen Ihnen als vertraulicher Ansprechpartner zur Verfügung. Sie erreichen uns per E-Mail unter caz@lfv.bayern.de. Falls Sie verschlüsselt mit uns kommunizieren möchten, finden Sie unsere PGP- und S/MIME-Schlüssel auf unserer Homepage unter Kontakt → Cyber-Allianz-Zentrum.

Mit freundlichen Grüßen

gez. Kergl