Dokumentation

Informationssicherheitshinweise zum Ukraine-Konflikt

Statusbericht

KLASSIFIZIERUNG	Öffentlich
STATUS	Freigegeben
EIGENTÜMER	r-tec IT-Security GmbH
VERSION	2.0
STAND	16.03.2022

Inhalt

1 Einleitung

Dieses Dokument beschreibt die bisherigen Erkenntnisse im Zusammenhang mit den Kriegshandlungen auf Ukrainischem Staatsgebiet und steht in Zusammenhang mit der erhöhten Warnlage von BSI und CERT-NRW. Es soll als Handreichung zur aktuellen Gefährdungslage und als Orientierungshilfe zur Absicherung von Kundennetzwerken dienen. Der Informationsstand entspricht jeweils dem auf dem Deckblatt angegebenen Stand der Berichterstattung externer Quellen.

2 Management Summary

Es besteht im Rahmen von Kriegshandlungen auf ukrainischem Staatsgebiet ein erhöhtes allgemeines Betriebsrisiko. Es wurde registriert, dass öffentlich erreichbare Ziele im Internet mit einer deutlich erhöhten Frequenz und Tiefe untersucht (allg. „Scans“) werden, als es sonst üblich ist. Bei den Untersuchungen handelt es sich nach externen Quellen vermutlich um Angreifer-Gruppierungen, die mit dem russischen Staat in Verbindung gebracht werden.

Es konnten sehr zielgerichtete und gut gemachte Phishing-Kampagnen beobachtet werden. Die Maßnahmen im Bereich E-Mail Security sollten nochmals auf Wirksamkeit überprüft werden.

Aufgrund einer Empfehlung des BSI sollte in Betracht gezogen werden, Sicherheitssoftware des Herstellers Kaspersky zeitnah durch andere Lösungen zu ersetzen.

Bislang konnte keine Ausnutzung unbekannter Lücken, z.B. Zero-Day-Lücken, festgestellt werden. Die obligatorischen Maßnahmen im Bereich der IT-Sicherheit (Zonierung, Firewall, Patch & Updatemanagement, Log Management, IDS, etc.) scheinen bislang wirkungsvoll zu sein.

In Bezug auf den vorgenannten Bereich der Untersuchung konnte beobachtet werden, dass Computersysteme im Einzugsgebiet der Ukraine nach einer erfolgreichen Kompromittierung durch spezialisierte Software (sog. „Wiper“) unbrauchbar gemacht werden. Die sonst weit verbreitete Methode, Daten mittels Ransomware zu verschlüsseln und Geld für die Entschlüsselung zu erpressen, kommt hierbei nicht zum Einsatz.

3 Analyse der Bedrohungslage

Bei der Untersuchung verfügbarer Informationen ist aufgefallen, dass es bislang keine Berichte darüber gibt, dass Computersysteme mit unbekannten Sicherheitslücken angegriffen werden. Daher ist davon auszugehen, dass der Schutz mit bekannten Mitteln wirkungsvoll möglich ist.

Es konnte beobachtet werden, dass seit dem 24. Februar 2022 Scans nach öffentlich erreichbaren Ports bzw. Diensten über das gesamte Internet stattfinden. Dessen Intensität geht deutlich über die normale Intensität, wie Sie täglich durch z.B. Suchmaschinen wie shodan.io erzeugt wird, hinaus. Für erkannte Dienste folgt ein intensiver Scan nach Verwundbarkeiten, sogenannte Vulnerability-Scans. Die hierbei erkannten Informationen zu Sicherheitslücken können für spätere Angriffe auf die betreffenden Computersysteme verwendet werden.

Wie bereits erwähnt, wird mit dem Rollout einer destruktiven Schadsoftware erheblicher Schaden angerichtet. Es gibt jedoch bislang keine Erkenntnisse auf einen Einsatz außerhalb der Ukraine.

Aufgrund diverser, professionell gestalteter Phishing-Kampagnen, die durch russische Hackergruppen durchgeführt werden, besteht derzeit ein hohes Risiko für eine Kompromittierung über den E-Mail-Weg.

Weiterhin ist aktuellen Berichten zu entnehmen, dass Akteure derzeit Multi-Faktor-Authentication (MFA)-Systeme, die eine selbstständige Registrierung für Benutzer ermöglichen (Selbstregistrierung), gezielt suchen und angreifen.

3.1 Best Practices für den Umgang mit destruktiver Malware

Wie bereits erwähnt, kann destruktive Malware eine direkte Bedrohung für den täglichen Betrieb eines Unternehmens darstellen und die Verfügbarkeit kritischer Anlagen und Daten beeinträchtigen. Unternehmen sollten ihre Überwachungsmöglichkeiten prüfen und Ihre Fähigkeiten in den Bereichen Planung, Vorbereitung, Erkennung und Reaktion auf ein solches Ereignis überprüfen.

Der Einsatz eines Incident-Response Dienstleisters erscheint hierbei als eine sinnvolle Option.

3.1.1 Potenzielle Verbreitungsvektoren

Malware kann sich über gängige Kommunikationsmittel verbreiten, z. B. über Dateien, die per E-Mail und Sofortnachrichten verschickt werden, über Trojaner, die von Websites heruntergeladen werden, und über infizierte Dateien, die über Peer-to-Peer-Verbindungen heruntergeladen werden. Malware kann ebenfalls von einem externen Angreifer aktiv („Hacking“) in Computersysteme des Opfers eingebracht werden. Malware versucht, bestehende Schwachstellen in Systemen auszunutzen, um sich unbemerkt und einfach Zugang zu verschaffen.

Die Malware ist in der Lage, eine große Anzahl von Systemen anzugreifen und kann über mehrere Systeme in einem Netzwerk ausgeführt werden. Daher ist es für Unternehmen wichtig, ihre Umgebung auf atypische Kanäle für die Verbreitung von Malware in ihren Systemen zu untersuchen. Zu den zu prüfenden Systemen gehören:

- Unternehmensanwendungen - insbesondere solche, die über eine direkte Schnittstelle zu mehreren Hosts und Endpunkten verfügen und diese beeinflussen können. Übliche Beispiele sind:
    - Patch-Management-Systeme,
    - Systeme zur IT-Inventarisierung,
    - Fernwartungssoftware (typischerweise vom Helpdesk des Unternehmens verwendet),
    - Endpoint-Security,
    - Systeme, die den System- und Netzwerkadministratoren zugewiesen sind,
    - Zentralisierte Sicherungsserver und
    - Zentralisierte Dateifreigaben.

3.1.2 Weitere Bedrohungen

Auch wenn dies nicht nur für Malware gilt, können Hacker weitere Ressourcen gefährden, um die Verfügbarkeit wichtiger Daten und Anwendungen zu beeinträchtigen. Gängige Beispiele sind:

- Zentralisierte Speichergeräte
    - Potenzielles Risiko - direkter Zugriff auf Partitionen und Data Warehouses.
- Netzwerkgeräte
    - Potenzielles Risiko - Möglichkeit, falsche Routen in die Routing-Tabelle einzuschleusen, bestimmte Routen aus der Routing-Tabelle zu löschen, Konfigurationsattribute zu entfernen/zu ändern oder Firmware oder System-Binärdateien zu zerstören, wodurch die Verfügbarkeit wichtiger Netzwerkressourcen isoliert oder beeinträchtigt werden könnte.

3.2 Endpoint Security

Das BSI führt in einer Warnmeldung aus, dass "die Zuverlässigkeit" sowie die "authentische Handlungsfähigkeit" des Herstellers Kaspersky (u.A. Antiviren-Software) nicht gewährleistet werden kann.

"Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden."

Da nicht für die Zuverlässigkeit des Herstellers Kaspersky im Hinblick auf politisch motiviertes Einwirken garantiert werden kann, wird die Ablösung von Security Produkten dieses Herstellers empfohlen. [8]

4 Erkennung

4.1 Log Management

Das Implementieren eines zuverlässigen Log Managements ist essentiell. Ohne eine zentralisierte Erfassung und Überwachung von Logdateien sind Unternehmen nur begrenzt in der Lage, Vorfälle zu untersuchen oder das in dieser Empfehlung beschriebene Verhalten von Hackern zu erkennen. Abhängig von der jeweiligen Umgebung kann dies mit den folgenden Lösungen realisiert werden:

- Sentinel von M365.
- Splunk / GrayLog
- Tools von Drittanbietern wie Sparrow, Hawk oder das Azure Reporting Tool (CRT) von CrowdStrike, um Microsoft Cloud-Umgebungen zu überprüfen und ungewöhnliche Aktivitäten, service principals und Anwendungsaktivitäten zu erkennen.

4.2 SIEM

Ein Next-Generation SIEM kann nach Verhaltensanzeichen oder Netzwerk- bzw. Hostbasierten Artefakten bekannter russischer staatlich gesponserter TTPs (Terrorist Tactics, Techniques, and Procedures) suchen und eine Alarmierung vornehmen. In Kapitel 7.4 werden bekannte TTPs aufgelistet.

5 Gegenmaßnahmen

5.1 Liste der häufig angegriffenen Schwachstellen

Die nachfolgende Liste enthält Schwachstellen, die häufig bei Angriffen auf Computersysteme und Infrastruktur beobachtet werden konnten. Sie führt bekannte Schwachstellen auf und ist nicht abschließend.

CVE-2021-34527 Windows Print Spooler Vulnerability
CVE-2018-13379 FortiGate VPNs
CVE-2019-1653 Cisco router
CVE-2019-2725 Oracle WebLogic Server
CVE-2019-7609 Kibana
CVE-2019-9670 Zimbra software
CVE-2019-10149 Exim Simple Mail Transfer Protocol
CVE-2019-11510 Pulse Secure
CVE-2019-19781 Citrix
CVE-2020-0688 Microsoft Exchange
CVE-2020-4006 VMWare (note: this was a zero-day at time.)
CVE-2020-5902 F5 Big-IP
CVE-2020-14882 Oracle WebLogic
CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

Es wird empfohlen, sämtliche Perimetersysteme mittels eines externen Vulnerability-Scans zu überprüfen.

Durch den Einsatz eines regelmäßigen externen Vulnerability-Scans können die Perimeter dauerhaft auf Schwachstellen überprüft werden und Probleme können rechtzeitig erkannt werden.

5.2 Patch und Update Management

Wenn Hersteller bei Schwachstellen, die schon länger bestanden und bisher unbekannt waren, Patches veröffentlichen, sollten diese auch kurzfristig (24/7) und mit hoher Priorität installiert werden. Dazu sollten mindestens bei allen externen Systemen kurzfristig die verfügbaren Sicherheitspatches installiert werden, siehe mindestens Top-Schwachstellen (https://www.cisa.gov/known-exploited-vulnerabilities-catalog). Auch wenn die Empfehlung der Installation aller ausstehenden Sicherheitspatches sehr unspezifisch ist, ist der Aufwand hierfür sehr gering. Daher hat diese Maßnahme ein sehr hohes Nutzen/Aufwand-Verhältnis und minimiert die eigene Angriffsfläche erheblich.

Durch den Einsatz eines regelmäßigen internen Vulnerability-Scans können die eingesetzten internen Systeme dauerhaft auf Schwachstellen überprüft werden und Probleme rechtzeitig erkannt werden.

5.3 Härtung aller Systeme mit Zugriffsmöglichkeit von außen

Unternehmen verfügen in der Regel über eine Vielzahl von Systemen mit Außenanbindung, z. B. VPN, RDP, OWA, Exchange-Online, usw. Bei Ransomware-Angriffen wurden bereits in der Vergangenheit gezielt Mitarbeitende von Unternehmen auch privat angegriffen, um dann über deren sowohl privat als auch beruflich genutzte Passwörter ins Unternehmensnetz einzudringen. Daher sollten alle Logins mit Außenanbindung über eine Multi-Faktor-Authentifizierung (MFA) geschützt werden.

Eine Absicherung ist kurzfristig durch den Einsatz von YubiKeys möglich.

5.4 Erschwerung von Lateral Movement ins/innerhalb des internen Netzwerks

Eine Kompromittierung externer Systeme und Netze, z.B. einer DMZ, darf nicht zur Kompromittierung wichtiger interner Systeme führen. Es gilt, die Vertrauensbeziehungen zwischen diesen Systemen zu minimieren und verschiedene Accounts mit verschiedenen Passwörtern in den jeweiligen Netzen zu nutzen.

5.5 Firewall Systeme

Moderne Firewall-Systeme können über ein geeignetes Regelwerk vollautomatisch Angriffe erkennen und unterbinden. Sie lernen darüber hinaus auch in kürzester Zeit durch einen Thread Feed des Herstellers bislang unbekannte Angriffe und können diese wirkungsvoll unterbinden.

Insbesondere Zugriffe auf externe Systeme sollte diesbezüglich intensiv mit geeigneten Lösungen überwacht werden.

Der Einsatz eines modernen Firewall-Systems ist eine geeignete Schutzmaßnahme. Die Erweiterung durch einen Incident-Response Dienstleister ist eine gute Ergänzung zu technischen Schutzmaßnahmen.

5.6 E-Mail Security

Ein Banner mit einem Hinweis auf externe Herkunft einer E-Mail stellt einen wichtigen Baustein für eine wirkungsvolle E-Mail Security dar. Diese Maßnahme sollte durch den Einsatz geeigneter Werkzeuge oder Lösungen ergänzt werden. Ein einfacher SPAM-Filter ist nicht mehr ausreichend.

5.7 Multi-Faktor-Authentifizierung

Es sollte überprüft werden, ob die MFA-Lösung wirksam konfiguriert ist. Insbesondere die Selbstregistrierung für Mitarbeiter ohne aktives MFA-Token sollte zwingend deaktiviert sein.

6 Backup und Desaster Recovery

Im Rahmen einer Business Impact Analysis (BIA) werden Systemkomponenten charakterisiert, klassifiziert und bestehende Interdependenzen erfasst. Auf den so identifizierten geschäftskritischen Ressourcen einer Organisation (und der damit verbundenen Abhängigkeiten) sollten für den Fall, dass eine Organisation von destruktiver Malware betroffen ist, Desaster-Recovery-Maßnahmen in Betracht gezogen werden.

Um in einem Ernstfall schnell handlungsfähig zu sein, sollten einer Organisation folgende Ressourcen zur Verfügung stehen. Im Idealfall wird die Verwendung der Ressourcen im Rahmen von Übungsszenarien geschult und geprüft.

- Umfassendes Inventar aller unternehmenskritischen Systeme und Anwendungen:
  - Versionsinformationen,
  - System-/Anwendungsabhängigkeiten,
  - Systempartitionierung/Speicherkonfiguration und Konnektivität, und
  - Ansprechpartner von Anlagen/Kontaktstellen.
- Kontaktinformationen für alle wichtigen Mitarbeiter innerhalb der Organisation,
- Sicherer Kommunikationskanal für Wiederherstellungsteams,
- Kontaktinformationen für externe Ressourcen:
  - Kommunikationsanbieter,
  - Anbieter (Hardware/Software), und
  - Outreach-Partner/externe Beteiligte
- Nummern von Serviceverträgen - für die Inanspruchnahme von Anbieterunterstützung,
- Kontaktstellen für die organisatorische Beschaffung,
- Optical Disc Image (ISO)/Image-Dateien für die grundlegende Wiederherstellung von kritischen Systemen und Anwendungen:
  - Betriebssystem-Installationsmedien,
  - Service Packs/Patches,
  - Firmware, und
  - Anwendungssoftware-Installationspakete.
- Lizenzierungs-/Aktivierungsschlüssel für Betriebssysteme und abhängige Anwendungen,
- Diagramme zur Topologie und Architektur des Unternehmensnetzwerks,
- System- und Anwendungsdokumentation,
- Ausdrucke von Betriebschecklisten und Playbooks,
- Sicherungsdateien der System- und Anwendungskonfiguration,
- Datensicherungsdateien (vollständig/differentiell),
- Checklisten/Richtlinien für System- und Anwendungssicherheitsgrundlagen und -härtung, und
- Checklisten für System- und Anwendungsintegritätstests und Abnahmetests.

Durch den Einsatz externer Consulting Teams kann der IT-Betrieb in die Lage versetzt werden, adäquat auf Bedrohungen zu reagieren.

7 IOC

7.1 Angreifer im Untersuchungskontext

Siehe Quelle [7]

7.2 Schadsoftware HermeticWiper

HermeticWiper	Hashes
Win32 EXE	912342f1c840a42f6b74132f8a7c4ffe7d40fb77
Win32 EXE	61b25d11392172e587d8da3045812a66c3385451
Win32 EXE	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591

ms-compressed	Hashes
RCDATA_DRV_X64	a952e288a1ead66490b3275a807f52e5
RCDATA_DRV_X86	231b3385ac17e41c5bb1b1fcb59599c4
RCDATA_DRV_XP_X64	095a1678021b034903c85dd5acb447ad
RCDATA_DRV_XP_X86	eb845b7a16ed82bd248e395d9852f467

7.3 Schadsoftware PartyTicket

Ransomware PartyTicket	Hashes
PartyTicket Golang Ransomware	4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382

7.4 MITRE Matrix bekannter russischer APT-Gruppen

Tactic	Technique	Procedure
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.
	Phishing for Information [T1598]	Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Russian state-sponsored APT actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.

Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Russian state-sponsored APT actors have used cmd.exe to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.
Persistence [TA0003]	Valid Accounts [T1078]	Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Russian state-sponsored APT actors have conducted brute-force password guessing and password spraying campaigns.
	OS Credential Dumping: NTDS [T1003.003]	Russian state-sponsored APT actors have exfiltrated credentials and exported copies of the Active Directory database ntds.dit.
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Russian state-sponsored APT actors have performed “Kerberoasting,” whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.
	Credentials from Password Stores [T1555]	Russian state-sponsored APT actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.
	Exploitation for Credential Access [T1212]	Russian state-sponsored APT actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.
	Unsecured Credentials: Private Keys [T1552.004]	Russian state-sponsored APT actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Russian state-sponsored APT actors have used virtual private servers (VPSs) to route traffic to targets. The actors often use VPSs with IP addresses in the home country of the victim to hide activity among legitimate user traffic.

8 Quellen

[1] https://twitter.com/ESETresearch/status/1496614321442459655?cxt=HHwWjsC4tfiyhcUpAAAA

[2] https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

[3] https://zetter.substack.com/p/second-wiper-attack-strikes-systems?utm_source=url

[4] https://github.com/SentineLabs/yara/blob/main/APT_ZZ_Unknown_HermeticWiper.yar

[5] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

[6] https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

[7] https://github.com/Orange-Cyberdefense/russia-ukraine_IOCs/blob/main/OCD-Datalake-russiaukraine_IOCs-ALL.csv

[8] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html