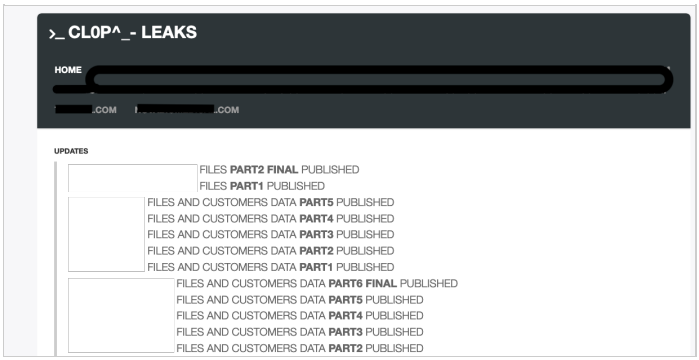
Aktueller Hinweis der Zentralen Ansprechstelle Cybercrime für die nds. Wirtschaft (ZAC)

Ransomware 2.0 - Aktuelles und Tipps

21.12.2020

Ransomware (Erpressungstrojaner, Verschlüsselungstrojaner) ist seit Jahren eine der größten Bedrohungen im digitalen Raum, sowohl für private als auch gewerbliche Nutzer und Netzwerke. Ein schwerer Vorfall kann nicht nur einen kompletten Datenverlust bedeuten, sondern auch die Veröffentlichung sensibler oder geheimer Daten.
In den letzten Monaten haben wir einen deutlichen Anstieg der Vorfälle in Niedersachsen beobachtet; diese Entwicklung spiegelt sich weltweit wider. Mit diesem Post wollen wir nochmal das Thema aufgreifen, aktuelle Information mitteilen und einige Vorschläge geben, wie Sie sich präventiv schützen können und was bei einem Vorfall zu beachten ist.

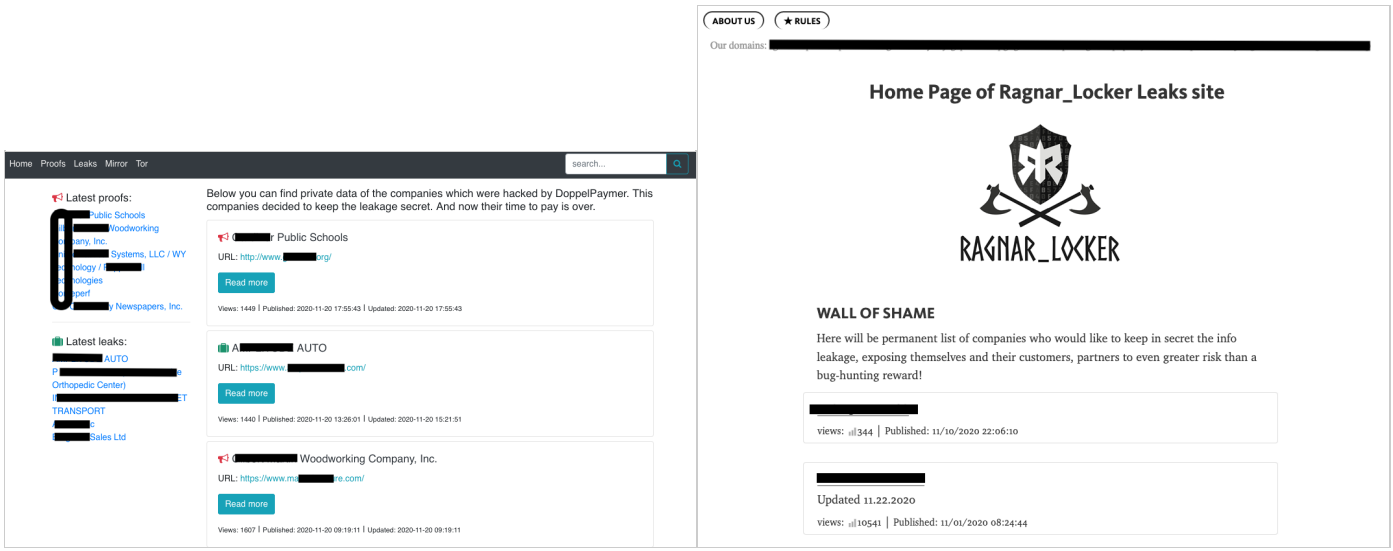


_CL0P^_ Ransomware Veröffentlichungen im TOR Netzwerk. Die von CL0P ausgespähten Daten werden bei Nichtzahlung hier veröffentlicht.

Aktuelles

Im Jahr 2020 ist ein Anstieg in der Anzahl der Ransomware-Vorfälle zu verzeichnen [1, 2]; das geforderte Lösegeld ist auch gestiegen [3].

- Infektionswege sind überall, wo eine Verbindung zum Internet möglich ist. Häufig erfolgt die Erstinfektion über eine schadhafte E-Mail; ebenso häufig in letzter Zeit sind Fernzugänge (RDP, VPN), z.B. für Home-Office, vertreten.
- In vielen Fällen ist eine mehrstufige Kompromittierung vorhanden: initiale Kompromittierung via E-Mail, Ausspähung von Daten, Ransomware wird zu einem späteren Zeitpunkt – manchmal Wochen bis Monate – nachgeladen.
- Bei solchen Angriffen sind oft verschiedene Tätergruppierungen aktiv: Der Zugang wird ermöglicht und weiterverkauft von Gruppe A, Gruppe B kauft sich Zugänge zu lukrativen Zielen und verschlüsselt die Systeme [4].
- Viele Ransomware-Varianten leiten jetzt Daten aus bevor sie verschlüsseln: wird nicht bezahlt, bleiben Ihre Daten verschlüsselt und die zuvor ausgespähten Daten werden zusätzlich im Internet (vorzugsweise Darknet bzw. TOR) veröffentlicht.
- Ausgespähten Daten werden nach Zahlung des Lösegeldes nicht immer gelöscht; manchmal werden Daten trotzdem von den Tätern veröffentlicht, manchmal erfolgt eine zweite Erpressung [5].



Wie bei CL0P betreiben weitere Ransomware Akteure wie DoppelPaymer und RagnarLocker auch sogenannte "shaming" Seiten im TOR Netzwerk.

Was Sie tun können

Ihre Aktionen vor und während eines Ransomware-Vorfalls können große Auswirkungen haben. Die folgenden Tipps – zusätzlich zu allgemeinen IT-Sicherheitsvorkehrungen wie Antiviren-Software, Backups, gute Passwörter und aktuelle Systeme – können Ihnen helfen, sich bzw. Ihre Organisation gegen einen Ransomware-Vorfall zu schützen.
Die meisten Tipps hier sind unabhängig vom Betriebssystem, allerdings beziehen sich einige direkt auf Windows Systeme und Netzwerke bzw. Active-Directory Umgebungen.

Im Voraus

Präventiv kann man einiges tun, um das Schadenspotential eines (Ransomware-) Angriffs zu begrenzen:

- *Backups:* Datensicherungen (Backups) sind eine der wichtigsten Maßnahmen und sollten regelmäßig erstellt und geprüft werden. Zusätzlich ist die 3-2-1-Regel zu empfehlen: drei Kopien des Backups auf zwei verschiedenen Medien, mit einer Offline-Kopie.
- *E-Mail-Filterung:* Nachrichten mit verdächtigem Inhalt (definierte Betreffe, Anhänge, Absender-Adressen, usw.) sollten direkt blockiert werden. Zusätzlich sollten Makros in über E-Mail empfangenen MS-Office Dateien deaktiviert werden [6]. Andere Mechanismen wie DMARC und SPF helfen, betrügerische Mails zu identifizieren. Nicht nur im Zusammenhang mit Ransomware, sondern auch bei den Betrugsvarianten CEO-Fraud bzw. Rechnungsmanipulation.
- *Aktuelle Systeme:* Systeme und Software regelmäßig aktualisieren, insbesondere die aus dem Internet zugänglichen Systeme [6].
- *Segmentierung:* das Netzwerk in kleinere Subnetzwerke einteilen, die nicht oder nur bedingt miteinander kommunizieren können, hilft dabei, die Ausbreitung von Schadsoftware (und somit die Schäden bei einem Vorfall) begrenzt zu halten.
- *Logs:* Die Auswertung von Netzwerk-Logdaten spielt eine zentrale Rolle bei einem Vorfall: damit lassen sich u.a. das Ausmaß des Vorfalls feststellen und ggf. den Infektionsweg ermitteln. Logging sollte regelmäßig erfolgen und Logs sollten sicher (und zentral) aufbewahrt werden. Überwachung der Logdaten auf Auffälligkeiten kann helfen, Angriffe frühzeitig zu erkennen [6, 7].
- *Blocklisten:* Netzwerkkommunikation mit bekannten Malware C2 (Command & Control) Servern kann anhand öffentlich verfügbarer Listen überwacht oder blockiert werden [7]. Solche Listen sind beispielsweise hier zu finden [8].
- *Kommunikationswege reduzieren:* die Menge der Kommunikationswege zwischen den einzelnen Systemen im eigenen Netzwerk (-segment) sollte auf das Nötigste reduziert werden: SMB, RDP, WMI, Windows Remote Management, Remote Powershell im internen Netzwerk unterbinden, wenn nicht zwingend notwendig. Diese Dienste und Ports sind die am häufigsten benutzten Verbreitungs- und Verteilwege innerhalb eines Netzwerkes [9].
  Sind solche Verbindungen doch notwendig, kann man gezielte Ausnahmen zulassen. Stellen Sie dann sicher, dass aktuelle (gepatchte) Versionen dieser Dienste verwendet werden.
- *Fernzugänge absichern:* sind Fernzugänge (wie RDP) vorhanden, sollten diese geschützt werden: Zwei-Faktor-Authentifizierung, Zugriff nur von bestimmten Quell-Adressen, Zugriff nur für bestimmte Nutzer*innen, Benutzung von VPN- bzw. RDP-Gateways [6, 7, 10].
- *Passwort Sicherheit:* Lokale-Administrator Konten werden häufig benutzt, um sich durch Netzwerke zu bewegen. Werden identische „Admin“ Passwörter über mehrere Rechner verwendet, wird das besonders einfach gemacht. Microsoft hat hierzu ein Security Advisory (KB2871997) [9].
- *Least-Privilege:* Konten mit erhöhten netzwerkweiten Rechten sollten nur von besonders dafür designierten Systemen benutzt werden. Eine Anmeldung mit solchen Konten auf normalen Endgeräten sollte nicht möglich sein. Ausführliche Information und SOLL-Regelungen zum Schutz des privilegierten Zugriffs in Active-Directory Umgebungen beschreibt Microsoft in [11].
- *Kritische Systeme* (z.B. Domain Controller) sollten bei einem Vorfall schnell isoliert werden können [9].
- *GPO Sicherheit:* Ransomware benutzt oft Group Policy Objects, um sich in einem Netzwerk auszubreiten. Konten, die mehrere GPOs verwalten, sollten besonders geschützt sein. Besonders geschützt sollten auch die GPOs sein, die Sicherheitseinstellungen für mehrere Geräte verwalten [9].

- *Externe Dienstleister berücksichtigen:* Hard- und Software von externen Dienstleistern, z.B. Telefonserver, die vom jeweiligen Provider verwaltet werden, sollten geprüft werden. In welchem Netzwerk (-segment) ist sowas zu finden? Verfügen diese Geräte (und somit ggf. die Verwalter dieser) über besondere Rechte im Netzwerk? Ein Vorfall bei einem externen Dienstleister kann in solchen Fällen für die eigene IT gravierende Folgen haben [6].
- *Planen und üben:* Das BSI empfiehlt Planbesprechungen und Übungen im Voraus, um auf einen Vorfall vorbereitet zu sein [7]. Hier können sogenannte Penetrationstests sehr hilfreich sein.
- *Versicherung:* eine Cyber-Versicherung kann sinnvoll sein, denn hier besteht oft die Möglichkeit, bei einem Vorfall technische Expertenhilfe schnell zu bekommen.

Während des Vorfalls

Bei einem laufenden Angriff ist die Eindämmung der Ausbreitung und somit der Schäden von größter Bedeutung. Die folgenden Sofortmaßnahmen sind zu empfehlen [12]:

- *Isolation:* alle (potenziell-) infizierten Systeme sind sofort zu isolieren: Netzwerkverbindung von betroffenen Systemen trennen. Nur wenn diese sich nicht vom Netzwerk trennen lassen sollten sie heruntergefahren werden.
- *Kritische Systeme schützen:* auch die kritischen Systeme können (und sollten) zu ihrer Sicherheit isoliert und erst nach Klarmeldung wieder in Betrieb genommen werden.
- *Out-of-Band Kommunikationen:* die fremde Überwachung der eigenen Aktivitäten und Kommunikationen (E-Mail) ist nach einem Vorfall möglich [6]; man sollte daher ein anderes Kommunikationsmittel benutzen, bis die Situation unter Kontrolle gebracht wurde.
- *Vorfall kommunizieren:* der Vorfall sollte intern klar kommuniziert werden. Auch die Mitteilung nach Außen (Kunden, Partner) kann sinnvoll sein, da manche Schadsoftware sich beispielsweise schnell im Namen des Opfers und unter Verwendung echten Mailverkehrs weiterverbreitet.
- *Prüfung privilegierter Konten:* Admin-Konten sollten geprüft werden: sind alle bekannt und legitim? Sind existierende Konten mit neuen Rechten erweitert worden? Sind sonst legitim erscheinenden Zugriffe zu ungewöhnlichen Zeiten erfolgt?
- *Infrastruktur prüfen:* die Infrastruktur sollte auch auf Unregelmäßigkeiten geprüft werden. Sind neue und/oder unbekannte Systeme, (virtuelle-) Maschine oder sonstige Geräte vorhanden?
- *Netzwerkverkehr prüfen:* ungewöhnliche Aktivitäten wie fehlgeschlagene DNS-Auflösungen, Datenverkehr in großen Mengen oder zu ungewöhnlichen Zeiten kann Hinweise auf Schadsoftware liefern [7]. Auch sind neue oder geänderte Freigaben im Netzwerk oft ein Zeichen eines Befalls.
- *Beweissicherung:* forensische Abbildungen sind für die Beweissicherung wichtig. Diese sind möglichst am Live-System anzufertigen, da nur so die flüchtigen Daten (wie aus dem Arbeitsspeicher) gesichert werden können. Hierfür ist oft spezielle Unterstützung notwendig, wie von einem IT-Dienstleister oder ggf. der Polizei.

Nach dem Vorfall

Ist der Angriff vorbei – egal ob er erfolgreich eingedämmt oder gar abgewehrt werden konnte – bleibt neben der Wiederherstellung der Systeme auch noch festzustellen, wie es zu dem Vorfall gekommen ist und wie man sich zukünftig dagegen schützen kann. Hierzu hat u.a. das BSI ausführliche Information bereitgestellt [12].

- Infizierte Systeme sollten als vollständig kompromittiert betrachtet werden [7]. Zugangsdaten, die auf diesen Systemen benutzt wurden, sollten auch als kompromittiert gelten.
- Kompromittierte Systeme sollten von „sauberen" Backups wiederhergestellt werden.
- Sind Backups nicht verfügbar, sollten die Systeme neu aufgesetzt werden.
- Verschlüsselte Daten sollten dabei aufbewahrt werden und nicht bei einer Neuinstallation oder Wiederherstellung überschrieben werden. Die Aufbewahrung ist wichtig, da manchmal Entschlüsselungstools – etwa nach erfolgreichen Ermittlungen oder Forschungsarbeit – kostenfrei veröffentlicht werden.
- Die Ermittlung des Infektionsweges ist enorm wichtig: nur so kann eine neue Infektion ausgeschlossen werden. Gefundene Lücken oder Schwachstellen müssen unmittelbar geschlossen werden. Oft ist spezialisierte Hilfe hier sinnvoll (Forensiker, IT-Sicherheitsexperten).
- Nach der Wiederherstellung oder Neuinstallation sollten die Systeme aktualisiert und gehärtet werden, bevor sie wieder im Netzwerk zugelassen werden [7].
- Wichtig ist, dass mit den sauberen Systemen neue Kennwörter gesetzt werden. Am besten ist es, alle auf den kompromittierten Systemen verwendeten Kennwörter neu zu setzen.
- In Active-Directory Umgebungen ist insbesondere das Problem von Golden Tickets zu beachten:

  > *„Angreifer mit Domänenadministrator-Rechten können das KRBTGT-Konto beeinträchtigen. Indem diese das KRBTGT-Konto verwenden, können sie ein Kerberos Ticket Granting Ticket (TGT) erstellen, das die Autorisierung für jede Ressource erteilen und den Ablaufzeitpunkt des Tickets auf einen beliebigen Zeitpunkt festlegen kann. Dieses gefälschte TGT wird als „Golden Ticket" bezeichnet und ermöglicht es Angreifern, dauerhaft die Kontrolle über das Netzwerk zu erhalten." [13]*

  Mehr Information – inklusive präventive und reaktive Maßnahmen – bietet das CERT-EU [14].

Hilfe beim Zurücksetzen des Kontos bietet auch Microsoft mit einem Powershell Skript [15].

Datenschutz und Meldepflichten

Ransomware-Vorfälle sind aktuell häufig mit der Ausspähung von Daten verbunden. Hier ein wichtiger Hinweis des BSI:

> *„Denken Sie an etwaige Meldepflichten etwa nach DSGVO, BSIG und anderen Gesetzen gegenüber Regulatoren. Beachten Sie außerdem etwaige Verpflichtungen aus vertraglichen Vereinbarungen." [12]*

In bestimmten Fällen sind sogar die betroffenen Personen direkt zu informieren [16].
Ausführliche Information zu Meldepflichten und -wegen bei Datenschutzverstößen bietet die Landesbeauftragte für den Datenschutz Niedersachsen [17].

Quellen

[1] BitDefender, „Mid-Year Threat Landscape Report 2020," 2020. [Online]. Verfügbar: https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf.

[2] PricewaterhouseCoopers LLP, „What is behind the increase in ransomware attacks this year?" 2020. [Online]. Verfügbar: https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

[3] TrendMicro, „2020 Midyear Cybersecurity Report," 26 August 2020. [Online]. Verfügbar: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report.

[4] FireEye, Inc, „Erpressung 2.0: Taktiken, Techniken und Prozesse bei Angriffen mit der Ransomware MAZE," 07 Mai 2020. [Online]. Verfügbar: https://www.fireeye.com/blog/de-threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html.

[5] Coveware, „Q3: Ransomware Demands Rise," 4 November 2020. [Online]. Verfügbar: https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

[6] Cybersecurity & Infrastructure Security Agency, „Ransomware Guide," September 2020. [Online]. Verfügbar: https://www.cisa.gov/publication/ransomware-guide.

[7] Bundesamt für Sicherheit in der Informationstechnik, „Ransomware - Bedrohungslage, Prävention & Reaktion 2019," 2020. [Online]. Verfügbar: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html.

[8] Abuse.CH, „URLHaus," 2020. [Online]. Verfügbar: https://urlhaus.abuse.ch/.

[9] FireEye, Inc, „Ransomware Protection and Containment Strategies," 30 Oktober 2020. [Online]. Verfügbar: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf.

[10] University of California, Berkeley, „Securing Remote Desktop (RDP) for System Administrators," [Online]. Verfügbar: https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/securing-remote-desktop-rdp.

[11] Microsoft, „Active Directory-Verwaltungsebenenmodell," 14 Februar 2019. [Online]. Verfügbar: https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material.

[12] Bundesamt für Sicherheit in der Informationstechnik, „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall," 28 Januar 2020. [Online]. Verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html

[13] Microsoft, „Domain Dominance Alerts," 26 Oktober 2020. [Online]. Verfügbar: https://docs.microsoft.com/de-de/defender-for-identity/domain-dominance-alerts.

[14] CERT-EU, „Kerberos Golden Ticket Protection," 2014. [Online]. Verfügbar: https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf.

[15] Microsoft, „Github | Microsoft | New KRBTGT Keys," [Online]. Verfügbar: https://github.com/microsoft/New-KrbtgtKeys.ps1.

[16] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, „Infoblatt „Meldung von Datenschutzverstößen"," [Online]. Verfügbar: https://www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/Infoblatt_Datenschutzverstoesse.pdf.

[17] Die Landesbeauftragte für den Datenschutz Niedersachsen, „Meldung von Datenschutzverstößen," [Online]. Verfügbar: https://lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/faq/meldung-von-datenschutzverstoeen-167312.html.

Permanenter Link zu diesem Artikel auf zac-niedersachsen.de:
https://zac-niedersachsen.de/artikel/55

Klicken Sie hier und abonnieren Sie unseren Newsletter.