TLP:GREEN

E-Commerce Fraud Forum
Aktuelle Bedrohungen aus CERT-Sicht

Robert Schischka <schisch@cert.at>

Top Targets (acc. ENISA)

1. Goverments
2. Health Care
3. Technological – Supply Chain
4. Finance (war früher Top 1)
5. Energy
6. Industrial
7. Transport

Ukraine 1: Dort

- Alle Russischen Cyberkräfte sind aktiv
  - Mehrere Wiper
  - Hack & Leak
  - Info-Operations
- Sabotage von KA-Sat traf UA hart
  - Koordination der Artillerie
  - Skylink hat hier geholfen

Ukraine 2: EU

- Initial nur lateral damage von Angriffen gegen UA assets
  - Wiper, KA-Sat
- Inzwischen:
  - Laufend DDoS Angriffe von Hacktivisten „Killnet“
  - Flughäfen, Eisenbahnen, Banken, Häfen
  - PL, DE, RO, CZ, LV, LT, IT, …
  - Wir erwarten in Zukunft mehr als „nur“ DDoS

Ukraine 3: Österreich

- Bis jetzt keine direkten Angriffe auf Österreich
- Sehr wohl aber Seiteneffekte:
  - Störung der Lieferketten
  - Sanktionen

AKTUELLE THEMEN

2022-05-20

Ransomware

- Massiv Vorfälle im Bereich KMU bis Großbetriebe und Behörden
- Datenextraktion und Erpressung mit Veröffentlichungsdrohungen mittlerweile „Standard“
- Angreifer oft über Wochen unentdeckt im Netz
- Backupsysteme werden gezielt identifiziert und angegriffen
- Restrore-Zeiten sind auch bei intaktem Backup ein Problem – insb. wenn die Basisinfrastruktur (AD, …) weg ist

Social Engineering

- „Dauerbrenner“ in alle Varianten
  - Phishing / Vishing / Smishing
  - CEO Fraud ….
- Die erfolgreichsten Angriffe bauen auf den Faktor Mensch – oft in Kombination mit technischen Angriffen, selten aber gänzlich OHNE menschliche „Mithilfe“

Log4j / log4shell

- Anfang Dez 2021
- „Feature“ in einer extrem weit verbreiteten Open Source Java Library
  - Technisch einfacher Fix, aber erst nach Tagen komplett umgesetzt
- Massiver Aufwand, das überall zu bereinigen
  - zB Bank hat 56.000 Arbeitsstunden in Bereinigung verbraucht!
- Global
  - Überraschend wenig Ausnutzung
  - Die meisten bekannten Fälle betrafen MobileIron
  - Warum?
    - Variabilität in den Systemen, die Log4j enthalten
    - Prevention Paradox?

Apropos Java

- Letztens Fehler in der Implementation des Elliptic Curve Signaturalgorithmus (ECDSA)
  - Ermöglicht trivial gefälschte Signaturen, die als korrekt behandelt werden
- Vom Impact her ganz spannend
  - Auf diese Crypto-Primitiven wurde viel aufgebaut
  - X.509 PKI, JWT, SAML, OIDC, WebAuthn
- Zum Glück wurde diese Java Implementation bei e-Gov Applikationen nicht breit verwendet

AD Certification Service

- Kein Bug, sondern häufiges Konfigurationsproblem
- Problem: Templates, die von der CA automatisch signiert werden, und die Zertifikats-Requests mit beliebigen Subject Alternative Names akzeptieren
- Bei TLS-based Authentication ergibt das eine triviale Privilege Escalation
- Wurde bei APT Fall in Österreich gesehen

Flubot

- Mobile Malware für Android
- Kann SMS „leise“ abfangen und weiterleiten
- Kunden die reklamieren dass sie SMS nicht erhalten sind pot. betroffen
- Erste Welle im Mai 2021 bei uns
  - Massiver Aufwand bei Telcos
  - Spannenden Regulatorische Fragen – darf man blocken / muss man Kunden schützen?
  - Hohe Kosten durch Massen-SMS
  - Kaum Schaden bei Banken – obwohl (anscheinend) auf SMS Abgreifen abgezielt
- Befallende Geräte sind nicht vom Betreiber nicht direkt erkennbar
- Schadsoftware lässt sich nur mit großem Aufwand wirklich restlos beseitigen

Flubot

- Katz und Maus Spiel:
  - C2 über DNS over HTTPs und öffentlichen Resolvern -> Mitigation durch Telcos schwierig
  - später: MMS statt SMS vermutlich weil MMS-Infrastruktur „eoL“ ist und dort Sperren schwierig rasch zu implementieren sind
  - Gute Nachricht: auch böse Jungs machen Fehler ;-)
  - Mittlerweile Infrastruktur von LAE übernommen und abgeschaltet

Emotet

- Nach einer Polizeiaktion vor einem Jahr war eine Zeit Pause
- Jetzt wieder zurück mit:
  - Malspam basierend auf echten Mailverläufen
  - Codeausführung primär über Microsoft Office Macros
  - Dokument nicht direkt angehängt:
    - In passwort-geschütztem ZIP File enthalten
    - Nur Link in email

Passwörter

- Passwort-Raten ist leider noch zu oft erfolgreich
- Password Spraying (gleiches Passwort bei vielen Users probieren)
- Credential Stuffing (User/Pw paare aus Leaks probieren)
- Unvollständige Umsetzung einer 2-Faktor Strategie, z.B.:
  - Webinterface mit username/pw, danach 2FA kann sich zum Durchprobieren eignen.
  - Benutzt werden die Funde dann bei einem anderen Interface, dass kein 2FA verlangt.

Follina-Schwachstelle (CVE-2022-30190): Neue Erkenntnisse, neue Risiken (9.6.2022)

Publiziert am 9. Juni 2022 von Günter Born

[English]Die seit Ende Mai 2022 bekannt gewordene Schwachstelle CVE-2022-30190 (Follina) in Windows entwickelt sich langsam zum Problembär. Die von Microsoft und hier im Blog beschriebenen Gegenmaßnahmen erscheinen nicht ausreichend. **Ergänzung:** Ich habe den aktuellen Diskussionsstand nachgetragen. Die Schwachstelle wird inzwischen zudem von der QakBot-Malware bei Phishing-Angriffen ausgenutzt. Weiterhin sind mir noch Informationen von Cato zur Schwachstelle zugegangen. Hier ein aktualisierter Überblick zum Sachstand.

Rückblick auf CVE-2022-30190

Bei der seit Ende Mai 2022 öffentlich gewordenen Schwachstelle CVE-2022-30190 (aka Follina) kann das Microsoft Support Diagnostics Utility (*msdt.exe*)über das *ms-msdt*:-Protokoll missbraucht werden, um bösartige Word-Dokumente (oder Excel-Arbeitsblätter) aus dem Web herunterzuladen. Der Angreifer kann die Sicherheitslücke ausnutzen, um Remote-Code mit den Rechten der aufrufenden Anwendung ausführen.

Ich hatte diesen Sachverhalt im Blog in den Beiträgen Follina: Angriff über Word-Dokumente und ms-msdt-Protokoll (CVE-2022-30190) und Follina-Schwachstelle (CVE-2022-30190): Status, Erkenntnisse, Warnungen & Angriffe aufgegriffen.

{* RESEARCH *}

Now Windows Follina zero-day exploited to infect PCs with Qbot

Data-stealing malware also paired with Black Basta ransomware gang

Jeff Burt

Thu 9 Jun 2022 // 00:29 UTC

3

Miscreants are reportedly exploiting the recently disclosed critical Windows Follina zero-day flaw to infect PCs with Qbot, thus aggressively expanding their reach.

The bot's operators are also working with the Black Basta gang to spread ransomware in yet another partnership in the underground world of cyber-crime, it is claimed.

This combination of Follina exploitation and its use to extort organizations makes the malware an even larger threat for enterprises. Qbot started off as a software nasty that raided people's online bank accounts, and evolved to snoop on user keystrokes and steal sensitive information from machines. It can also deliver other malware payloads, such as backdoors and ransomware, onto infected Windows systems, and forms a remote-

Fragen?

- https://www.cert.at/
- team@cert.at