Malware und Schwachstellen H1 2022

Ein Überblick über die Bedrohungslandschaft

Donnerstag, 27. Oktober 2022

Recorded Future®

Julian Kanitz
Lead Sales Engineer, DACH

Hello!

Julian Kanitz

Lead Sales Engineer DACH

@Recorded Future

Findet mich unter:

https://www.linkedin.com/in/juliankanitz

julian.kanitz@recordefuture.com

Index

- **Einführung**
- **Malware [H1 2022]**
  - Hartnäckigkeit bestimmt das erste Halbjahr
- **Schwachstellen [H1 2022]**
  - Dominierende Schwachstellen
- **Beobachtungen**
  - Top referenzierte Malware
  - Top referenzierte Schwachstellen
- **Ausblick H2 2022**

Recorded Future®

Einführung

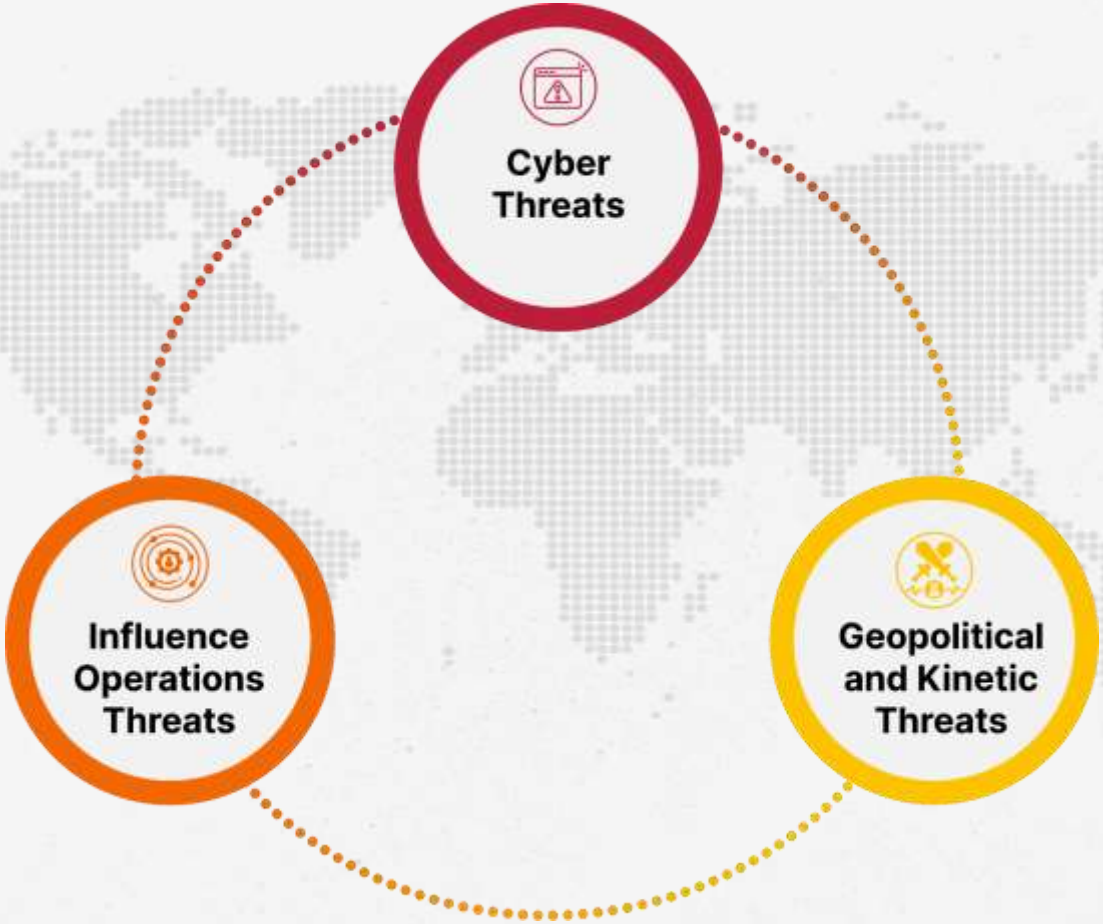
Recorded Future®

Index

- **Einführung**
- **Malware [H1 2022]**
  - Hartnäckigkeit bestimmt das erste Halbjahr
- **Schwachstellen [H1 2022]**
  - Dominierende Schwachstellen
- **Beobachtungen**
  - Top referenzierte Malware
  - Top referenzierte Schwachstellen
- **Ausblick H2 2022**

Recorded Future®

Die Bedrohungen konvergieren



Kontinuierliche und flächendeckende Abdeckung

Malware [H1 2022]

Recorded Future®

Index

- **Einführung**
- **Malware [H1 2022]**
  - Hartnäckigkeit bestimmt das erste Halbjahr
- **Schwachstellen [H1 2022]**
  - Dominierende Schwachstellen
- **Beobachtungen**
  - Top referenzierte Malware
  - Top referenzierte Schwachstellen
- **Ausblick H2 2022**

Recorded Future®

Malware [H1 2022]

Hartnäckigkeit bestimmt das erste Halbjahr

Infostealer

Wiper Malware

Ransomware

Malware [H1 2022]

Infostealer

Infostealer

- “Russian Market” wird mit kompromittierten Daten von Infostealern gefüttert, die darauf ausgelegt sind, sensible Daten von den Rechnern der Opfer zu identifizieren und zu exfiltrieren.
- “Raccoon Stealer” (vorübergehende Einstellung der Operationen im März 2022)
- “Threat Actors” wechselten zu Mars Stealer, MetaStealer, BlackGuard, RedLine & Vidar
- Ende des 1. Halbjahres 2022 tauchte Raccoon Stealer 2.0 wieder auf [Erneut steigende Popularität]

Malware [H1 2022]

Wiper Malware

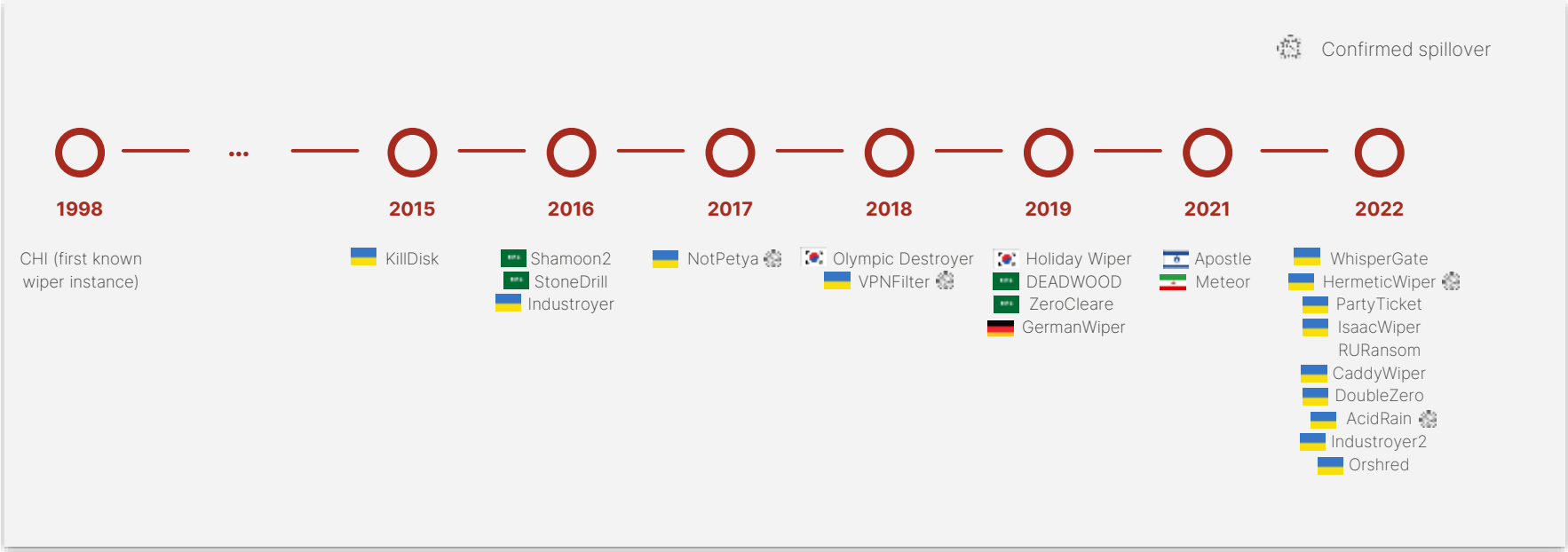
Wiper Malware

- Neue zerstörerische Malware (mit Ziel Ukraine)
- 9 verschiedene Varianten von Wiper-Malware, die für die russische staatlich geförderte Kriegsführung eingesetzt werden
- Weniger Zeit und weniger Ressourcen für die Entwicklung von Malware gegen wichtige geopolitische Ziele.
- Es wurde festgestellt, dass die 9 Varianten im Laufe der Zeit immer einfacher wurden, wobei die Entwicklung weniger Verschleierung und weniger Stufen zwischen den Varianten umfasste.

Malware [H1 2022]

Wiper Malware

Der Einsatz von Wiper-Malware steht in Zusammenhang mit geopolitischen Konflikten, wird immer ausgefeilter und hat das Potenzial, auf andere Länder überzugreifen.



Quelle: Recorded Future

Malware [H1 2022]

Ransomware

- Conti Ransomware griff die Regierung von Costa Rica an
- Die Conti Ransomware Group hat ihre “Extortion Infrastruktur” anschließend im Rahmen einer Auflösungsaktion abgeschaltet.
- Die produktivsten Betreiber sind diejenigen, die hinter den Ransomware-Familien Lockbit 3.0 und Hive stehen.
- FIN7 (finanziell motiviert) wurde von Recorded Future identifiziert, nachdem sie ein Cybersicherheitsunternehmen (Bastion Secure) gegründet hatten, um Tools für die Zeit nach der Ausbeutung (Carbanak) so einzusetzen, als wären es IT-Management- und Sicherheitsüberwachungs-Tools

Scwachstellen [H1 2022]

Recorded Future®

Index

- **Einführung**
- **Malware [H1 2022]**
  - Hartnäckigkeit bestimmt das erste Halbjahr
- **Schwachstellen [H1 2022]**
  - Dominierende Schwachstellen
- **Beobachtungen**
  - Top referenzierte Malware
  - Top referenzierte Schwachstellen
- **Ausblick H2 2022**

Recorded Future®

schwachstellen [H1 2022]

Dominierende Schwachstellen

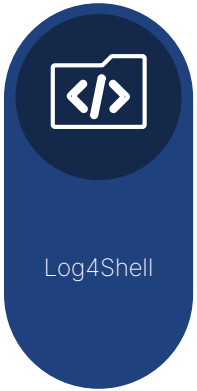
Log4Shell

ProxyShell

Follina

Schwachstellen [H1 2022]

Apache Log4J - Log4Shell [CVE-2021-44228]



- Von 2021 bis 2022 war eines der meistdiskutierten Themen im Bereich der Cybersicherheit Log4Shell, die einfach auszunutzende Schwachstelle in der Log4J-Software von Apache.
- Erst im Juni 2022 gab es wieder Nachrichten über Cyberangreifer, die Log4Shell ausnutzen.

Schwachstellen [H1 2022]

Microsoft Exchange Server - ProxyShell

CVE-2021-34473
CVE-2021-34523
CVE-2021-31207

- Die Ausnutzung einer Reihe von Sicherheitslücken, die unter dem Namen ProxyShell bekannt sind und Microsoft Exchange betreffen, war ebenfalls eine ständige Bedrohung durch mehrere “Threat Actors”.

- Bei der Untersuchung von Schwachstellen haben wir festgestellt, dass Cyberkriminelle bevorzugt eine kleine Gruppe bekannter Schwachstellen angreifen, bei denen sie sicher sein können, dass sie auf den Systemen der Opfer vorhanden sind.

Schwachstellen [H1 2022]

Microsoft Windows - Follina [CVE-2022-30190]

- "Follina" ist der Name für die Sicherheitslücke im Microsoft Support Diagnostic Tool (MSDT).
- H1 2022 begann mit Antworten auf "Log4Shell", und "Follina" definierte das Ende der ersten Jahreshälfte.
- Es stellt einen neuen Bereich der Ausnutzung von Microsoft Windows-Systemen ohne Einsatz von bösartigen Makros dar.
- Es wird Microsofts Entscheidung sein, wie die Zukunft von Windows Malware (maldocs) aussehen wird. Entweder Makro-basiert oder auf Windows-Utilities basierend.

Beobachtungen

Recorded Future®

Index

- **Einführung**
- **Malware [H1 2022]**
  - Hartnäckigkeit bestimmt das erste Halbjahr
- **Schwachstellen [H1 2022]**
  - Dominierende Schwachstellen
- **Beobachtungen**
  - Top referenzierte Malware
  - Top referenzierte Schwachstellen
- **Ausblick H2 2022**

Recorded Future®

Malware [H1 2022]

Top referenzierte Malware

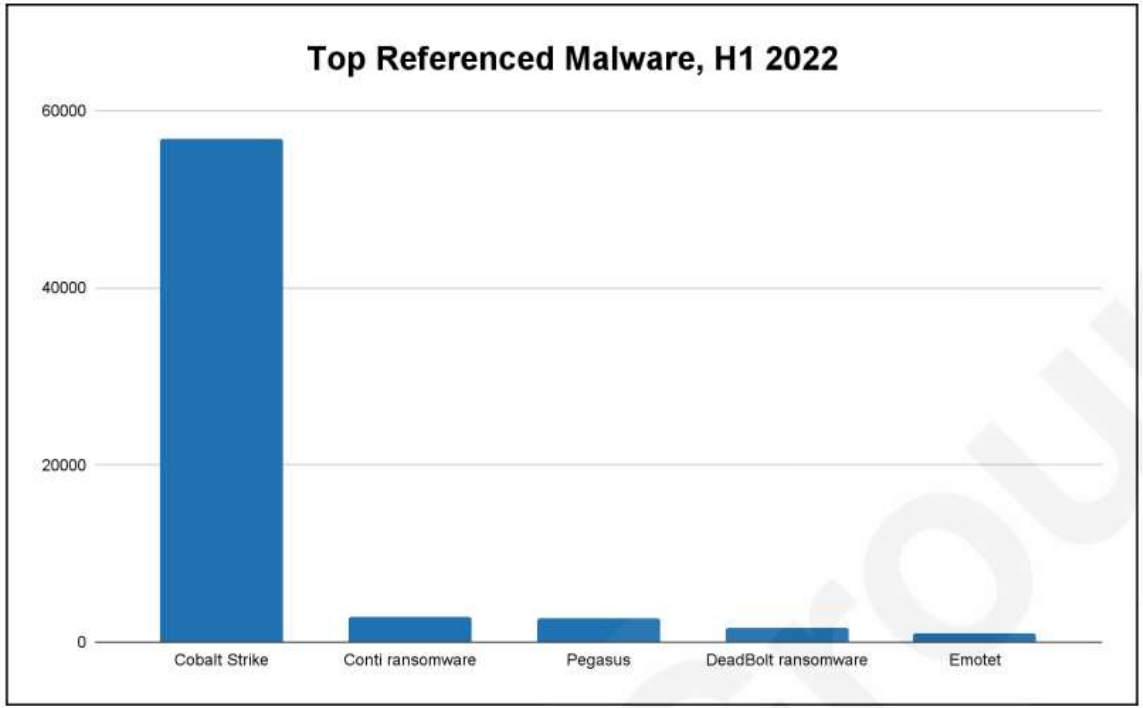


Figure 1: *Malware appearing in the most references to reported cyberattacks, H1 2022 (Source: Recorded Future)*

Vulnerabilities [H1 2022]

Top referenzierete Schwachstellen

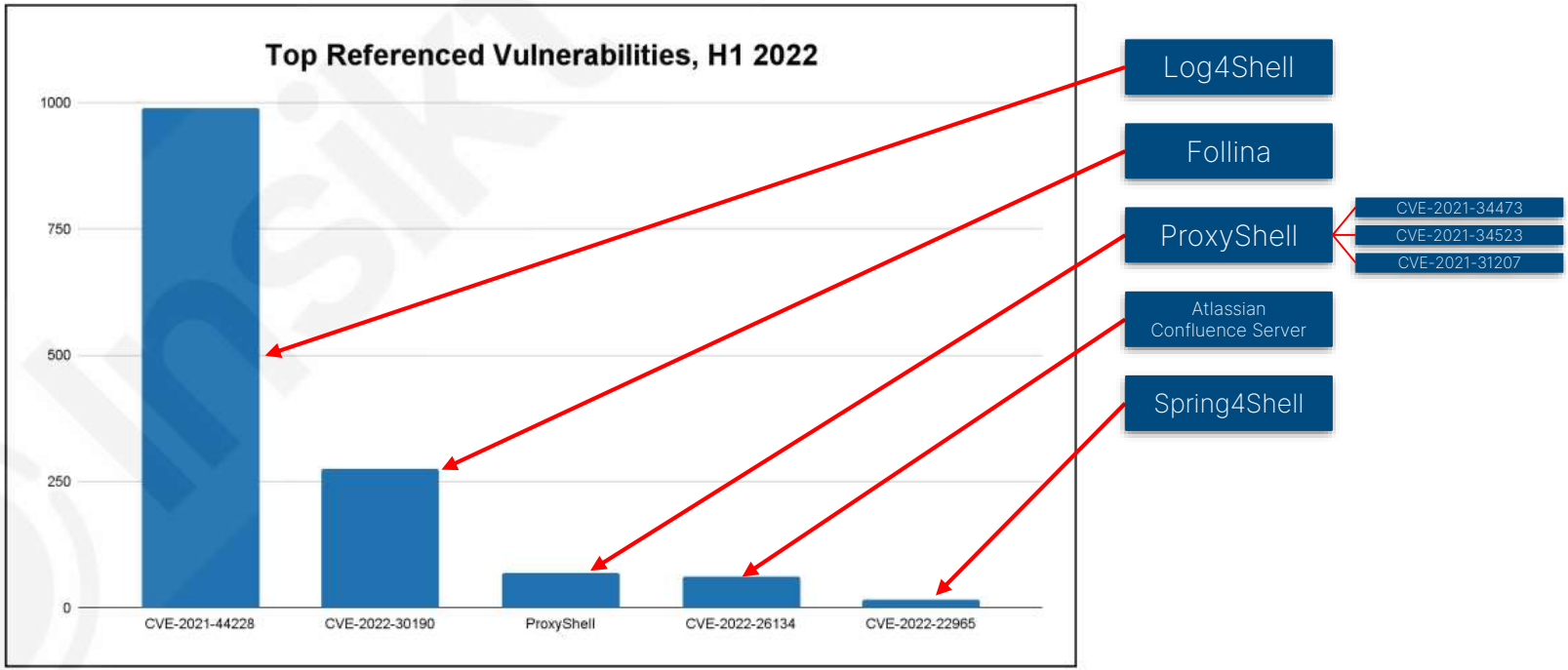


Figure 2: *Vulnerabilities appearing in the most references to reported cyberattacks, H1 2022. ProxyShell includes 3 distinct vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207). (Source: Recorded Future)*

Ausblick [H2 2022]

Recorded Future®

Index

Outlook H2 2022

- Persistenz von Ransomware-Operationen, kriminellen Foren, Botnet-Einsatz und Zero-Day-Ausnutzung.
- Diebstahl von Zugangsdaten und “Browser fingerprints”. Es ist wahrscheinlich, dass wir eine radikale Veränderung der Malware und der kriminellen Märkte erleben werden - mehr und ausgefeiltere Stealer-Malware.
- Mehr kriminelle Versuche zur Umgehung von Einmal-Passwörtern (OTP) und MFA als Richtung der Malware-Entwicklung.
- Prognosen über die Zukunft des Krieges liegen außerhalb unseres Wissens, aber es ist wahrscheinlich, dass wir mehr disruptive Angriffe sehen werden, solange die bestehende russische Regierung an der Macht bleibt.

Fragen?

Julian Kanitz
@ Recorded Future

Recorded Future®

Fragen?

Julian Kanitz
@ Recorded Future

Recorded Future®