

Cyberangriffe seit dem Ukraine-Krieg - die neuesten Trends

Jeannette Baasner-Lukath

Manager Systems Engineering
Öffentliche Auftraggeber

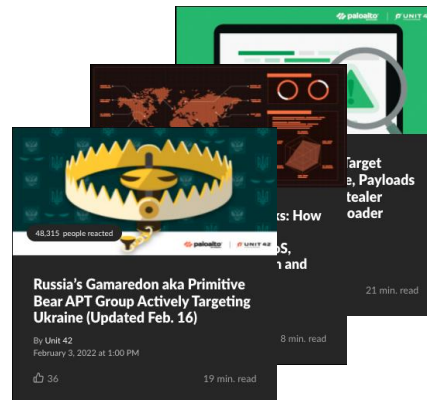
Telefon
Email

+49.160.98962072
jbaasner@paloaltonetworks.com



Beobachtete Ereignisse und Trends um den Beginn des Ukraine-Kriegs

Beobachtete Ereignisse von Unit 42



Nov

Dec

Jan

Feb

Mar

Gamaredon cyber activity **attributed** to Russian FSB

U.S. Government publishes **advisory** of Russian threats to US Critical Infrastructure

WhisperGate destructive malware impacts Ukraine Government

Defacement of Ukraine Government Websites

Cyber Partisans compromise Belarus state run railways

APT29 - Two NATO country MFAs

AgainstTheWest Operation Ruble

APT29 - 4 Western Ministry of Foreign Affairs

DDoS, Hermetic Wiper, and Defacement attacks

ContiLeaks reveals Conti groups internal comms

Scammers take advantage of news for fraud

CaddyWiper impacts small number of Ukrainian systems

Deepfake presidents used in Russia-Ukraine war

Beobachtete Trends



Wiper Malware

Beispiele

- WhisperGate
- HermeticWiper
- IsaacWiper

Nicht als Ransomware, sondern zu rein destruktiven Zwecken.



Angriffe auf Regierungs- Webseiten

Beispiele

- DDoS Angriffe
- OctoberCMS

Generelle Störung, Des-Information und psychologische Einflussnahme.



Gezielte Langfrist- Kampagnen

Beispiele

- Gamaredon
- Industroyer

“Spillover” auf westliche Organisationen findet bereits statt.

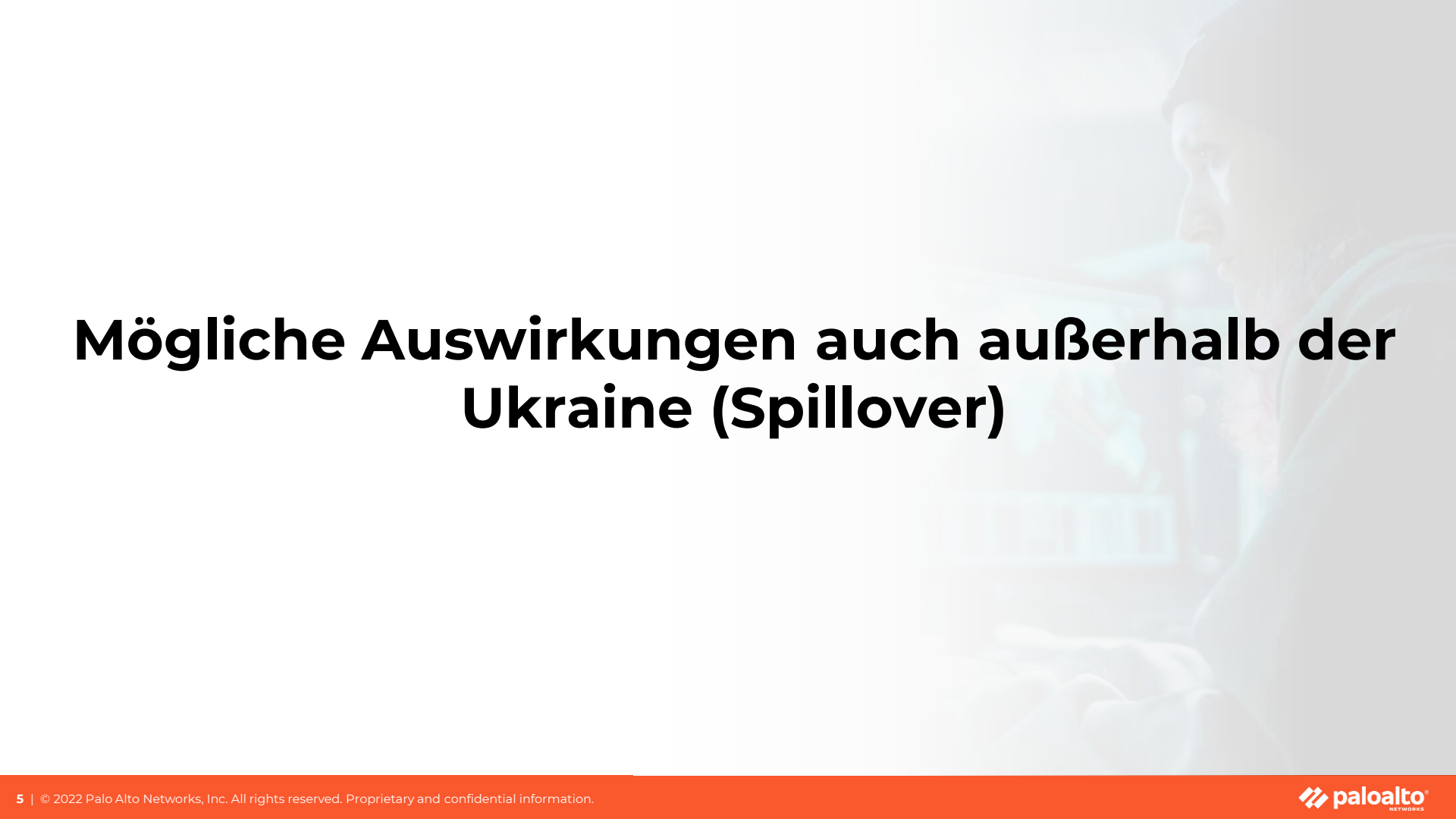


Bevölkerung als Ziel von Angriffen

Beispiele

- Scamming
- Fake Donation
- Deepfake

Verunsicherung und Ausnutzung der Lage zu finanziellen und politischen Zwecken.



Mögliche Auswirkungen auch außerhalb der Ukraine (Spillover)

Mögliche Auswirkungen außerhalb der Ukraine



Destructive Malware

DDoS Angriffe

Angriffe gegen
Kritische Infrastrukturen



Zusätzliche Auswirkungen
auf Unternehmen, die in
oder für die Ukraine tätig
sind
(e.g., NotPetya)



Ideologisch oder
nationalistisch motivierte
Angriffe

Handlungsempfehlungen



Russland-Ukraine-Krise - Ziele und Ressourcen der Krisenreaktion

MONITOR

Überwachung von Cyberangriffen auf die Ukraine und andere Organisationen



Palo Alto Networks is closely monitoring developments in Ukraine

Palo Alto Networks is closely monitoring the rapidly evolving cyber activity related to Russia and Ukraine. We continue to release new Unit 42 threat intelligence, deploy protections for our customers, and are actively collaborating with our partners in industry and governments to share our analysis and findings based on our global threat network.

Protecting our customers is our highest priority. In line with warnings by multiple governments, we are also diligently preparing for any cyberattacks that may spread beyond Ukraine. We will continuously update this resource center with the latest cybersecurity information including research, best practices, intelligence, and threat intelligence from the Unit 42 blog. We are standing by and ready to assist our customers as needed.

As of 4/1/2022, the following indicators have been identified

2150	318
Domains	Binaries
265	681
IPs	URLs

PROTECT

Implementierung von Produkten & Maßnahmen zum Schutz vor bekannten Bedrohungen



Technology

Palo Alto Networks provides a full portfolio of products and threat intelligence, and we've reinforced relevant capabilities:

- **Threat Prevention:** Added coverage for the October/CMS vulnerability CVE-2021-32668, exploited in the WhisperGate attacks.
- **WildFire:** Improved detection of **WhisperGate**, which disables Windows Defender and other specific malware families like HermeticWiper that are used by Russian threat groups.
- **Advanced URL Filtering:** Blocked hundreds of new malicious domain names, IP addresses and URLs.
- **Cortex XDB:** Updated defenses and added signatures to block newly discovered malware, including HermeticWiper, in order to protect the entire attack surface across cloud, networks, endpoints, users and critical infrastructure.
- **Cortex Xpanse:** Our automated Attack Surface Management (ASM) platform provides a complete and accurate inventory of your global Internet-facing assets to discover, evaluate and mitigate security issues.
- **Prisma Cloud CWP:** Identify and update out-of-date packages and known exploited vulnerabilities.
- **Prisma Cloud WAAS:** Block OWASP Top 10 attacks on web applications and APIs and prevent attacks that leverage the new CVE based on virtual patching.
- **Prisma Cloud CSPM:** Identify IOC used by attackers using threat detection. Prioritize critical web-facing vulnerabilities using True Network Exposure.

EDUCATE

Informationen austauschen, um Bewusstsein für und Kenntnisse über die aktuellen Bedrohungen zu schärfen



PREPARE

Unterstützung von Organisationen bei der Bewertung und Vorbereitung auf Bedrohungen



Security Consulting and Incident Response Services

Our research indicates that recent attacks have used ransomware or a destructive attack that poses as ransomware (i.e., **WhisperGate**).

- **Proactive Assessments:** Unit 42 cyber risk management consultants are ready should you wish to be better prepared.
- A **Ransomware Readiness Assessment** can help identify potential weaknesses in your response playbook and identify any ongoing or historical indicators of compromise.
- **Incident Response:** Unit 42 IR services can help companies of any size investigate and remediate potential threat actor activity. If you have been breached or have an urgent matter, contact us [here](#).



RESPOND

Unterstützung bei der Reaktion auf aktive Bedrohungen und bei der Wiederherstellung



Are you under attack?

Unit 42's Incident Response team will quickly help you understand the nature of the attack, work with your team to contain and remediate the breach, and get you back to business fast.

If you have been breached or have an urgent matter, please call the Unit 42 Incident Response team or fill out the form to get in touch immediately.*

- North America Toll-Free: +1 866 486 2842 (+1 866 424 UNITY42)
- UK: +44 20 3213 3660
- EMEA: +31 20 299 3130
- APAC: +65 6983 8730
- Japan: +81 50 1290 0300

If you have cyber insurance or legal counsel, you can request for Unit 42 to serve as your incident response team. Unit 42 is on over 70 cyber insurance panels as a preferred vendor.

Danke

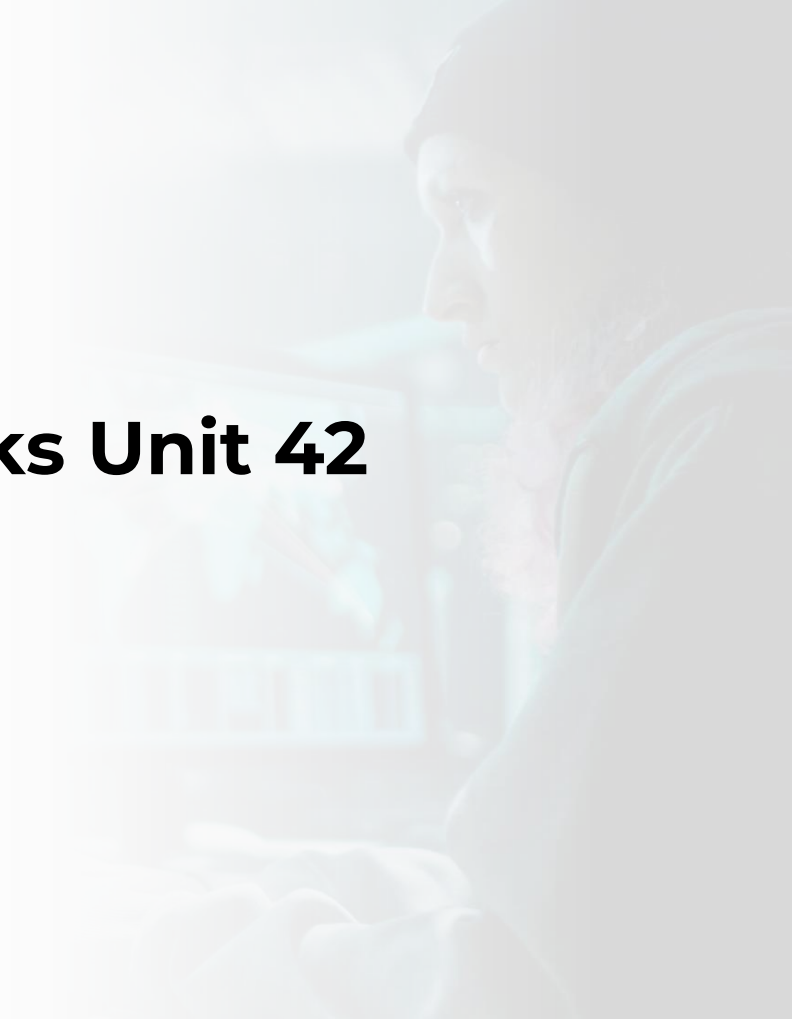


Jeannette Baasner-Lukath
Manager Systems Engineering
Öffentliche Auftraggeber

Telefon
Email

+49.160.98962072
jbaasner@paloaltonetworks.com

Palo Alto Networks Unit 42



Unit 42: Experts in Threat Research



200+ Threat Researchers



Reverse engineering



10+ years of historical malware analysis growing by 30M samples a day



Threat modeling



Multiple awards for vulnerability research



Depth and Breadth of Telemetry



85k+ customers



500BN events per day from endpoint, network, cloud



1k+ Incident response engagements per year



Across multiple verticals



Partnerships and Open Source Data



Open source gathering



75+ third party feeds



Cyber Threat Alliance, 6M observables/month



Law enforcement, government, military partnerships