UNIT 42
BY PALO ALTO NETWORKS

Cyberangriffe seit dem Ukraine-Krieg - die neuesten Trends

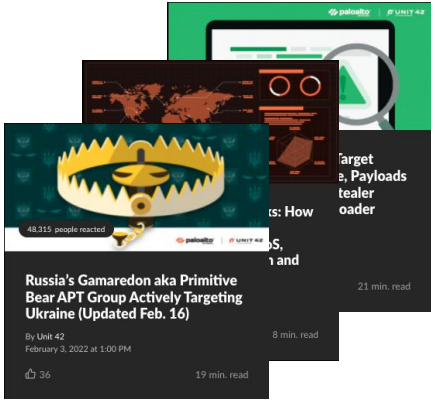
Jeannette Baasner-Lukath
Manager Systems Engineering
Öffentliche Auftraggeber

Telefon +49.160.98962072
Email jbaasner@paloaltonetworks.com

paloalto NETWORKS

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

Beispiele
- WhisperGate
- HermeticWiper
- IsaacWiper

Nicht als Ransomware, sondern zu rein destruktiven Zwecken.

Beispiele
- DDoS Angriffe
- OctoberCMS

Generelle Störung, Des-Information und psychologische Einflussnahme.

Beispiele
- Gamaredon
- Industroyer

“**Spillover**” auf westliche Organisationen findet bereits statt.

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

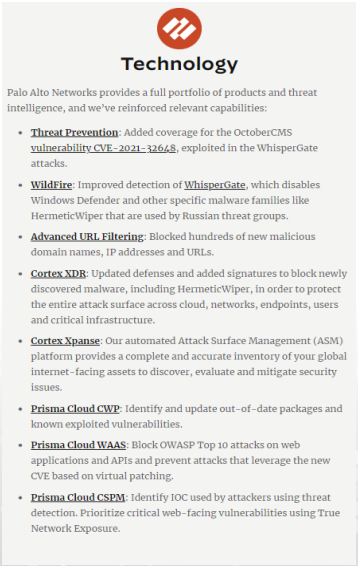
Russland-Ukraine-Krise - Ziele und Ressourcen der Krisenreaktion

MONITOR

Überwachung von Cyberangriffen auf die Ukraine und andere Organisationen

PROTECT

Implementierung von Produkten & Maßnahmen zum Schutz vor bekannten Bedrohungen

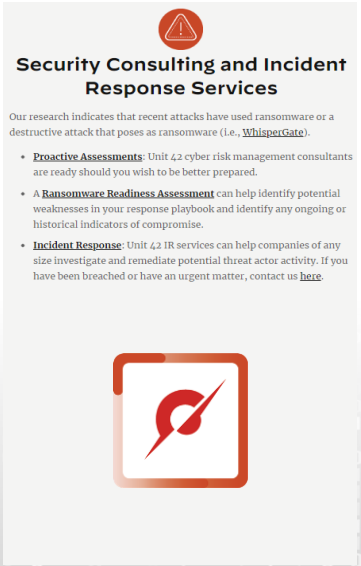


EDUCATE

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

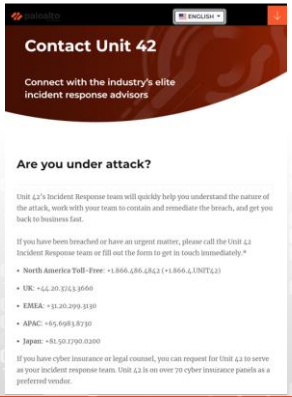
PREPARE

Unterstützung von Organisationen bei der Bewertung und Vorbereitung auf Bedrohungen



RESPOND

Unterstützung bei der Reaktion auf aktive Bedrohungen und bei der Wieder-herstellung



UNIT 42
BY PALO ALTO NETWORKS

Danke

Jeannette Baasner-Lukath
Manager Systems Engineering
Öffentliche Auftraggeber

Telefon +49.160.98962072
Email jbaasner@paloaltonetworks.com

paloalto NETWORKS

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

