elastic security labs

Global Threat Report 2022

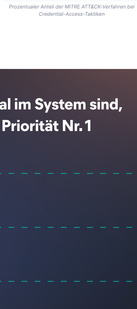
Infografik

Woher kommen die Bedrohungen?

Der „Global Threat Report" 2022 von Elastic Security Labs zeigt anhand von Lösungstelemetriedaten Bedrohungsphänomene und Trends auf und gibt Empfehlungen, um Organisationen aller Art dabei zu helfen, sich auf die Zukunft vorzubereiten. Wir haben ein paar der Erkenntnisse für Sie zusammengestellt.

Praktische Clouds werden sicher, wenn schlechte Standardwerte geändert werden.

Bei fast 41 % der Credential-Access-Alerts wurde versucht, Zugriffstoken für Anwendungen zu stehlen, statt an andere Credential-Informationen heranzukommen.



Prozentualer Anteil der MITRE ATT&CK-Verfahren bei Credential-Access-Taktiken

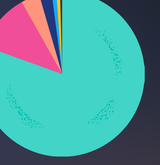
Wenn Angreifer erst einmal im System sind, ist Credential Access Priorität Nr. 1

Prozentualer Anteil der einzelnen MITRE ATT&CK-Taktiken für Cloud-basierte Erkennungs-Alerts

Kommerzielle Software wird als Waffe genutzt

Ursprünglich für Red Teams entwickelte Malware wird heute gegen Organisationen eingesetzt.

CobaltStrike war die am häufigsten beobachtete bösartige Binärdatei bzw. Payload für Windows-Endpoints, gefolgt von AgentTesla und RedLineStealer.



Open Software ist nicht so sicher, wie Sie denken.

Top 10 der Linux-Malware und Payloads, die die Zunahme der BPFDoor-Aktivitäten illustrieren

Trojaner sind nach wie vor eine der beliebtesten Arten, Deliverables als Waffe zu nutzen

Gute Nachrichten: Endpoint-Security funktioniert

Angreifer, die es auf Endpoints abgesehen haben, setzen zur Umgehung von Schutzmaßnahmen verstärkt auf eine Vielzahl unterschiedlicher Methoden. Dieses Jahr haben wir 50 unterschiedliche Verfahren zum Infiltrieren von Endpoints beobachtet, die nicht funktioniert haben.

Verfahren	Anteil an den Signalen
Masquerading	44,29 %
System Binary Proxy Execution	30,00 %
Access Token Manipulation	12,32 %
Process Injection	7,62 %
BITS Jobs	4,74 %
Trusted Developer Utilities Proxy Execution	0,90 %
XSL Script Processing	0,66 %
Impair Defenses	0,65 %
Exploitation for Defense Evasion	0,64 %
System Script Proxy Execution	0,13 %
Modify Registry	0,03 %
Indicator Removal on Host	0,01 %

Alle Informationen zu den Erkenntnissen von Elastic Security Labs finden Sie im „Global Threat Report" 2022