cat out

Blueliv.

Diebstahl Von Zugangsdaten Im Fokus

JUNE 2018

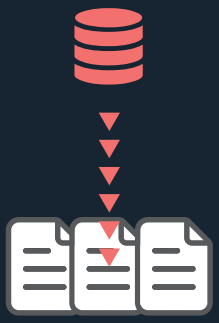
Cyberkriminelle stehlen Zugangsdaten mit einer Vielzahl von Techniken, Taktiken und Verfahren.

Der Markt für kompromittierte Zugangsdaten ist extrem ausgebreitet und bietet ein hohes Potenzial.

Zugangsdaten von Unternehmen werden verwendet, um Organisationen zu verletzen und vertrauliche Informationen zu stehlen.

Von **Erpressung** und **Lösegeld**, Verkauf von sensiblen Informationen bis hin zu Betrug, das Endziel ist normalerweise, von ihrem Angriff zu profitieren.

Viele illegale Aktivitäten für **finanziellen Gewinn** hängen vom Erhalt von Zugangsdaten ab: die **'Schlüssel'**, die Türen zu Organisationen und ihren Kunden öffnen.



81 % von Hacking-bedingten Vergehen nutzen entweder **gestohlen** oder **schwache Passwörter** und alle Sicherheitsprodukte der Welt können eine Organisation nicht schützen, wenn die Kriminellen **den richtigen Schlüssel haben**, um die Tür zu öffnen.

Es gibt eine wachsende Industrie im Ökosystem der Internetkriminalität, die sich darauf konzentriert, gültige Zugangsdaten mithilfe verschiedener Mechanismen und Tools zu erhalten. **Alle diese Tools und Dienstleistungen können kostengünstig im Untergrund erworben werden.**

Malwareinfektion

Phishing

Mittelsmann

DNS-Hijacking

Sicherheitslücken

Brute-Force

Zugespielte Datenbanken

Social Engineering

Cyberkriminelle, die Zugangsdaten stehlen, nutzen diese normalerweise nicht selbst.

Es gibt boomende Märkte, wo sich Käufer und Verkäufer über die Konditionen einigen.

Man braucht nur eine einzige korrekte Anmeldeinformation, um Zugang zu einer Organisation zu erhalten und Chaos zu verursachen..

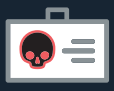
Sobald die Zugangsdaten erfasst wurden, können sie je nach Typ auf unterschiedliche Weise verwendet werden.

Verletzung der Datensicherheit

Nutzt Unternehmenskonten als Türöffner für schwere Einbrüche.

VIP Verkörperung

Verkörperung von Unternehmens-VIPs in Social Media oder E-Mail-Kommunikation, um den Ruf zu schädigen oder betrügerische Finanztransaktionen anzuweisen.



Gefährdung von Konto & Identitätsdiebstahl

Verkörperung echter Kunden zum Diebstahl von Waren und Dienstleistungen, von persönlichen Adressen über E-Mail bis hin zu Streaming-Sites.

Betrug

Ausführung von betrügerischen Transaktionen in Finanzinstituten.

Selbst bei kompromittierten Kundendaten übernimmt in der Regel das Unternehmen, das den Service oder die Ware anbietet, die Kosten der betrügerischen Transaktion.

Qualität vor Quantität: Cyberkriminelle schätzen neue Zugangsdaten von Unternehmen wesentlich mehr als Tausende von Datensätzen aus unzuverlässigen Lecks.

Kommerzielle Anmeldedaten von VIPs oder Vermögenswerten sind die wertvollsten, ganz oben auf der Liste. Der Preis für diese Anmeldedaten ist "Wert pro Transaktion".

Die Frische der Daten - der Zeitraum, seitdem die Daten kompromittiert wurden - ist entscheidend.

Je frischer die Daten, desto höher die Chance, dass der Cyberkriminelle sein finanzielles Ziel erreichen kann. Noch besser ist es, wenn die Zugangsdaten kompromittiert wurden, ohne den betroffenen Benutzer zu alarmieren (z. B. Malware, die sich nach dem Sammeln der erforderlichen Daten selbst entfernt).

Anmeldedaten werden von Cyberkriminellen nur selten in "Echtzeit" verwendet.

Wenn sie nicht durch gezielte Angriffe kompromittiert werden, benötigen Cyberkriminelle Zeit, um die riesigen erfassten Datenmengen zu analysieren, die "besten" Zugangsdaten herauszufiltern und die Daten zu verkaufen, wenn sie diese nicht selbst nutzen wollen.

Je schneller Unternehmen kompromittierte Zugangsdaten erkennen, desto besser.

Das frühzeitige Erkennen von Zugangsdaten - innerhalb weniger Tage nach ihrer Gefährdung - kann die Auswirkungen eines Angriffs massiv reduzieren.

Alle Branchen sind von Diebstahl von Zugangsdaten betroffen.

Es gibt eine Vielzahl von Möglichkeiten, wie Cyberkriminelle unabhängig von der Branche Gewinne erzielen können.

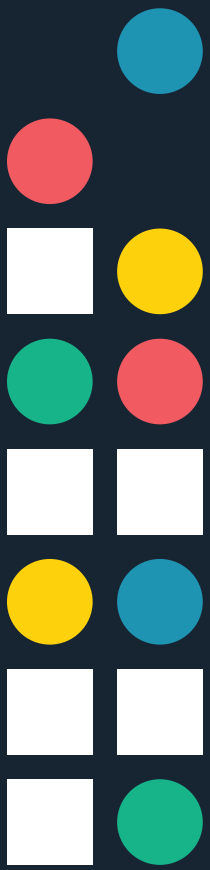
GDPR bedeutet, dass Persönliche Identifizierbare Informationen (PII) für Cyberkriminelle attraktiver werden.

Sie können höhere Beträge für die Nichtveröffentlichung der Informationen verlangen, da Unternehmen von der Gesetzgebung hart getroffen werden.

Der Lebenszyklus von Zugangsdatendiebstahl

Das Verständnis des Lebenszyklus von Zugangsdaten ist der erste Schritt, um die Tür für Cyberkriminelle zu schließen.

Basierend auf der Expertise von Blueliv in diesem Bereich, ist das Ziel dieses Berichts, zu erklären, wie das Ökosystem von Zugangsdaten funktioniert, wie Cyberkriminellen diese erhalten, wie sie verarbeitet und monetarisiert werden und welche Maßnahmen Organisationen ergreifen können, um den Diebstahl von Zugangsdaten zu verhindern und abzuschwächen.



1.Erfassen

- Malware-infektion
- Phishing
- Mittelsmann
- DNS Hijack
- Vulnerabilities
- Brute-Force
- Zugespielte Datenbanken
- Social Engineering

2.Filterung & Extrahierung

- Paneele
- Email
- FTP
- IRC
- Hacking-Werkzeuge Kundenspezifische Programme
- Sonstige

3.Validierung

- Botnetze
- Kontoprüfer
- Manuell

4.Profitieren

- Zugangsdaten-Handel
- Direkte Nutzung

Gestohlene Bank- und Social-Network-Zugangsdaten werden am häufigsten verwendet, gefolgt von E-Mail- und Web-Service-Providern, Einzelhändlern und E-Commerce.

62%
Wachstum der Zahl der georteten kompromittierten Zugangsdaten aus europäischen Ländern (Vergleich Jan-Mai 2017-2018)

½
Europa und Russland beherbergen seit Januar 2017 die Hälfte der Opfer von geortetem Identitätsdiebstahl weltweit.

Preislisten für Zugangsdaten:

Einzelhändler
$9

Partnersuche
$3.50/$8.50

Soziale Netzwerke
$1.50/$9

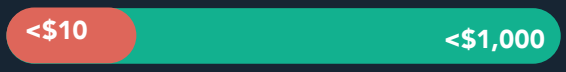
Zahlungsanbieter
$2-$100
(je nach Saldo)

Online-Streaming-Dienste
$2/$9

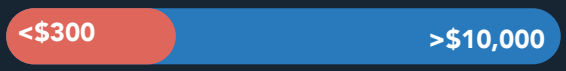
Firmenkonten
Privat geschlossen

Bankwesen

Konten mit leerem Saldo werden ebenfalls verkauft, und zwar zu einem Preis von ca. 4 $.



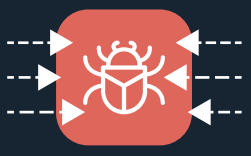
Kosten von Zugangsdaten
<$10, wenn der Saldo unter $1.000 liegt.



Kosten von Zugangsdaten
>300 Dollar, wenn der Saldo höher als 10.000 Dollar ist.

Kosten von Zugangsdaten
>25.000 Dollar, wenn der Saldo höher als 500.000 Dollar ist.

Top-Diebstahltechniken:


Malware


Phishing


Schwachstellen

Pony, KeyBase und LokiPWS sind die aktivsten Diebe.

Ein C2-Dieb bleibt durchschnittlich 60 Tage aktiv.

Die Verteilung von LokiPWS ist im vergangenen Jahr um mehr als 300 % angestiegen

Vermeidung von Datendiebstahl:

Sicherheitsbewusstsein & Bildung

Host-/Netzwerk-Erkennung von Malware-Infektionen

Überwachungsleistungen für Datendiebstahl

Über cat out

Die cat out gmbh - Gesellschaft für Informationssicherheit - bietet individuelle Beratung und Vermittlung von Softwarelösungen mit Schwerpunkt und Blick auf den Schutz und Monitoring von unerwünschtem Verlassen von Daten und Informationen aus den Unternehmen.

Besondere Aufmerksamkeit gilt hier der Kombination aus technischen Softwarelösungen und organisatorischen Maßnahmen um Wirtschaftsspionage und Datenverlust durch Cyber Angriffe sowie Mitarbeiterverhalten - gewollt oder ungewollt - zu verhindern und zu analysieren.

Basierend auf Partnerschaften renommierter internationaler Cybersecurity Softwarehersteller bietet Ihnen die "cat out" die Voraussetzung zur "Best Practice " Umsetzung der Themen : Threat Protection , End Point Protection and Response, Data Leak und Data Loss Prevention.

Die "cat out" kooperiert mit ausgewiesenen Spezialisten um für die verschiedenen Themen Lösungen zu finden und umzusetzen.

cat-out.com

info@cat-out.com

https://www.linkedin.com/company/cat-out/

Über Blueliv

Blueliv ist einer der führenden Anbieter von Cyber-Bedrohungsinformationen in Europa. Wir durchforsten das Open Web, Deep Web und das Dark Web, um Unternehmen neue, automatisierte und umsetzbare Bedrohungsinformationen zu liefern und ihre Netzwerke von außen nach innen zu schützen.

Die skalierbare, cloud-basierte Technologie von Blueliv verwandelt globale Bedrohungsdaten in ausgeklügelte, relevante Informationen. Wir ermöglichen es Unternehmen, Zeit und Ressourcen zu sparen, indem wir die Reaktion auf Vorfälle beschleunigen und benutzerfreundliche Beweise bereitstellen, die für alle Ebenen innerhalb von Cybersecurity-Operationen zugänglich sind.

Unsere Pay-as-you-need-Lösung liefert einen beschleunigten, vorausschauenden Überblick über die Bedrohungssituation in Echtzeit. Wir glauben nicht an einen Einheitsansatz und arbeiten zusammen, um eine modulare Lösung zu konfigurieren, die auf Ihre Bedürfnisse zugeschnitten ist, indem wir separate Module verwenden, die alle von unserem erstklassigen internen Analystenteam unterstützt werden.

Blueliv wurde zum Gartner Cool Vendor und Go-Ignite Gewinner ernannt und ist seit mehreren Jahren Mitglied der FS-ISAC.

blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/unternehmen/blueliv