HP WOLF SECURITY

Bedrohung durch Cyberkriminalität wächst: Warum das Dark Web die Gefahrensituation verschärft und wie man sich dagegen wehren kann

EIN HP WOLF SECURITY REPORT

Inhalt

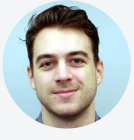
Beitragende zu diesem Report

ALEX HOLLAND
Hauptautor, HP Senior Malware Analyst

JOANNA BURKEY
HP Chief Information Security Officer

DR. IAN PRATT
Global Head of Security for Personal Systems bei HP

BORIS BALACHEFF
Chief Technologist for Security Research and Innovation bei HP Labs



PATRICK SCHLÄPFER
HP Malware Analyst

MICHAEL CALCE
Früher als Hacker "MafiaBoy" bekannt, heute Chairman des HP Security Advisory Boards, CEO von DecentraWeb und Präsident von Optimal Secure

DR. MIKE MCGUIRE
Senior Lecturer in Kriminologie an der University of Surrey in UK und Experte auf dem Gebiet der Cyber-Security

ROBERT MASSE
Mitglied des HP Security Advisory Boards und Partner bei Deloitte

JUSTINE BONE
Mitglied des HP Security Advisory Boards und CEO von MedSec

Zusammenfassung

Das Dark Web hat aus Cyberkriminalität ein lukratives Business noch nie gesehenen Ausmaßes gemacht.

Durch die Bereitstellung einer anonymen Online-Umgebung, in der Cyberkriminelle zusammenarbeiten, sich organisieren, ihre Fähigkeiten trainieren und illegale Geschäfte einrichten können, hat sich die Cyberkriminalität im Dark Web zu einer vielschichtigen, rufschädigenden Dienstleistungsbranche entwickelt.

Dieser Bericht, der von HP Wolf Security in Zusammenarbeit mit Forensic Pathways[1] und mit Sicherheitsexperten aus Industrie und Wissenschaft erstellt worden ist, zeigt auf, wie Cyberkriminelle heute auf professioneller Basis agieren und leicht zu startende Malware- und Ransomware-Angriffe auf Grundlage von “Software as a Service” angeboten werden. Infolgedessen sind nun auch Personen mit rudimentären IT-Kenntnissen in der Lage, Cyberangriffe auf Ziele ihrer Wahl zu starten.

"Der digitale Wandel hat sowohl Angriffs- als auch Abwehrmaßnahmen hochgerüstet, wobei es zunehmend einfacher ist, an beides zu kommen – siehe die Beliebtheit von "As-a-Service"-Angeboten. Dies hat bösartige Aktivitäten so weit demokratisiert, dass komplexe Angriffe, die ein hohes Maß an Wissen und Ressourcen erfordern – und die früher nur von APT-Gruppen (Advanced Persistent Threats) durchgeführt werden konnten – nun für eine weit größere Menge an Bedrohungsakteuren zugänglich sind", sagt Alex Holland, Senior Malware Analyst im Threat Research Team von HP Wolf Security – und Autor dieses Berichts.

Diese komplexen Angriffe werden auch durch ständige Datenlecks begünstigt, was dazu führt, dass Milliarden persönlicher Zugangsdaten auf Dark-Web-Märkten für kleinste Summen erhältlich sind. Viele der Malware-Varianten und Exploits, die in Ransomware- und Datenerpressungsangriffen Verwendung finden, werden für weniger als 10 Euro verkauft. Es ist vielleicht keine Überraschung, dass das FBI die Verluste durch Cyberkriminalität in den USA allein im Jahr 2021 auf erstaunliche 6,9 Milliarden Dollar schätzt.[2]
Auch wenn es den Anschein hat, als stünden die Chancen für Cyberverteidiger schlecht, gibt es doch enorme Möglichkeiten, seinen Schutz zu verbessern. In vielerlei Hinsicht geht es einfach

> "Die digitale Transformation hat beide Seiten der Kluft zwischen Angriff und Verteidigung in die Höhe getrieben."
>
> Alex Holland, leitender Malware-Analyst bei HP Analyst at HP Inc.

darum, die Grundlagen zu beherrschen. Während die Auswirkungen von Cyberangriffen zugenommen haben und sich Tools und Techniken weiterentwickelt haben, sind die wichtigsten Angriffsvektoren relativ unverändert geblieben. Dies bietet den Verteidigern die Möglichkeit, ganze Klassen von Bedrohungen zu bekämpfen und die Widerstandsfähigkeit zu verbessern.

5 wichtige Fakten zu Cyberkriminalität

11 Milliarden

Heute enthält eine einzige Website zur Meldung von Datenschutzverletzungen über 11 Milliarden Datensätze[3]

Über

3/4

der angebotenen Malware kostet weniger als 10 Dollar

Benutzerdefinierte Exploits kosten

1.000- 4.000$

92%

der cyberkriminellen Marktplätze bieten Streitbeilegungsdienste an und alle erlauben Käufern und Verkäufern, Bewertungen zu hinterlassen

91%

der Marktplatz-Anzeigen für Exploits liegen unter 10 $

Abschnitt 01

Von Hobby-Hackern zu Cyber-Syndikaten – Wie sich finanziell motivierte Cyberkriminalität entwickelt hat

Die Blaupause für Cybercrime-Gemeinschaften

Mitte der 1990er Jahre gab es eine florierende Hackersubkultur, die weltweit über Internet Relay Chat (IRC) kommunizierte.[4] Anfangs wollten die Hacker mit ihren technischen Fähigkeiten angeben. Doch mit dem Dotcom-Boom erkannten viele, dass sich damit Geld verdienen ließ.

> "Früher musste man selbst etwas herausfinden und mit seinen technischen Fähigkeiten angeben, um wahrgenommen zu werden. Heute programmiert nur noch eine kleine Minderheit von Cyberkriminellen, den meisten geht es nur ums Geld – und die Einstiegshürde ist so niedrig, dass fast jeder ein Bedrohungsakteur sein kann. Das sind schlechte Nachrichten für Unternehmen."

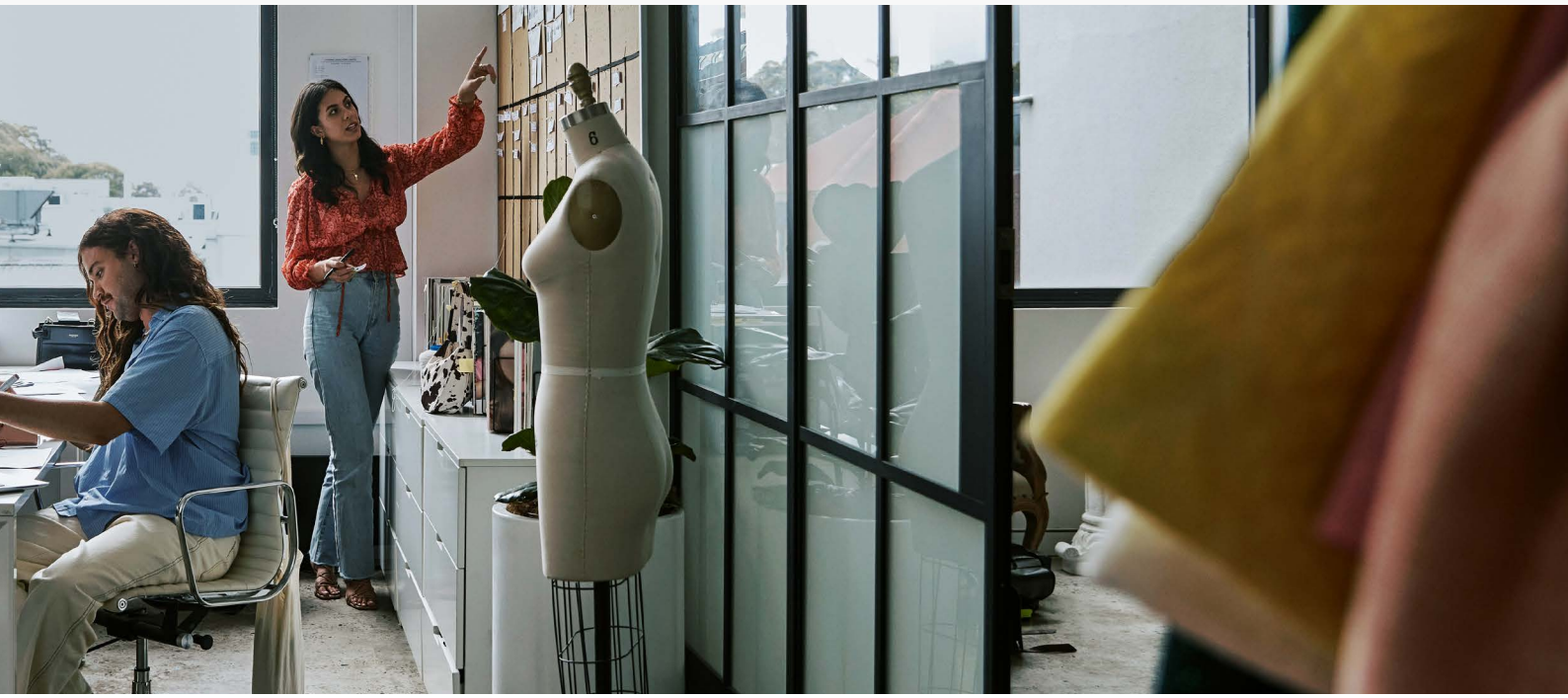
Michael Calce, Vorsitzender des HP Security Advisory Boards und ehemaliger Hacker "MafiaBoy".

KEY FACTS

Es bildeten sich globale Hacker-Communities, die Exploits und Angriffstechniken austauschten.

Gruppen und Einzelpersonen tauschten ihre Errungenschaften aus und demonstrierten so ihre technischen Fähigkeiten.

Die Angriffe waren in der Regel nicht finanziell motiviert.



DIY-Cybercrime-Kits öffnen den Markt für Cyberkriminalität

Die Einführung von Malware-Kits führte zu einer Senkung des erforderlichen Qualifikationsniveaus. Diese "Einzelkämpfer" hatten jedoch kaum Möglichkeiten, ihre Operationen zu erweitern, bis sie begannen, zusammenzuarbeiten und ihre Fähigkeiten zu bündeln. Dies führte dazu, dass sich Hacker auf die Perfektionierung verschiedener Teile der Angriffskette spezialisierten – sei es das Eindringen in Systeme, die Entwicklung von Malware oder das Waschen von gestohlenem Geld und Kryptowährungen.

KEY FACTS

Standardisierte Malware-Kits senkten die Einstiegshürden.

Cyberkriminelle begannen, ihre Kräfte in neuen Netzwerken zu bündeln und sich auf bestimmte Bereiche zu spezialisieren.

Die Monetarisierung konzentrierte sich auf Betrug und zielte auf Online-Banking-Nutzer statt auf Unternehmen ab.

IM FOCUS

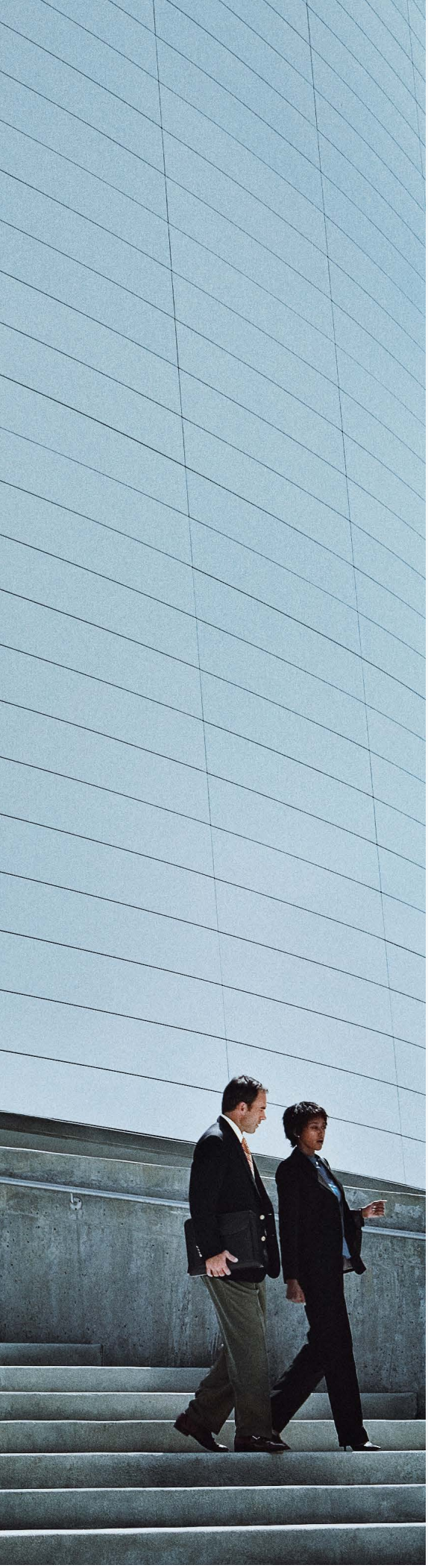
ZeuS and SpyEye

Das ZeuS DIY-Bankentrojaner-Kit ermöglichte es, ein Netzwerk kompromittierter Computer – ein sogenanntes Botnet – einzurichten, zu hosten und zu befehligen. Ziel war es, in betrügerischer Absicht Bargeld von vielen Online-Bankkonten abzuheben oder Kreditkartennummern zu erlangen. [5]

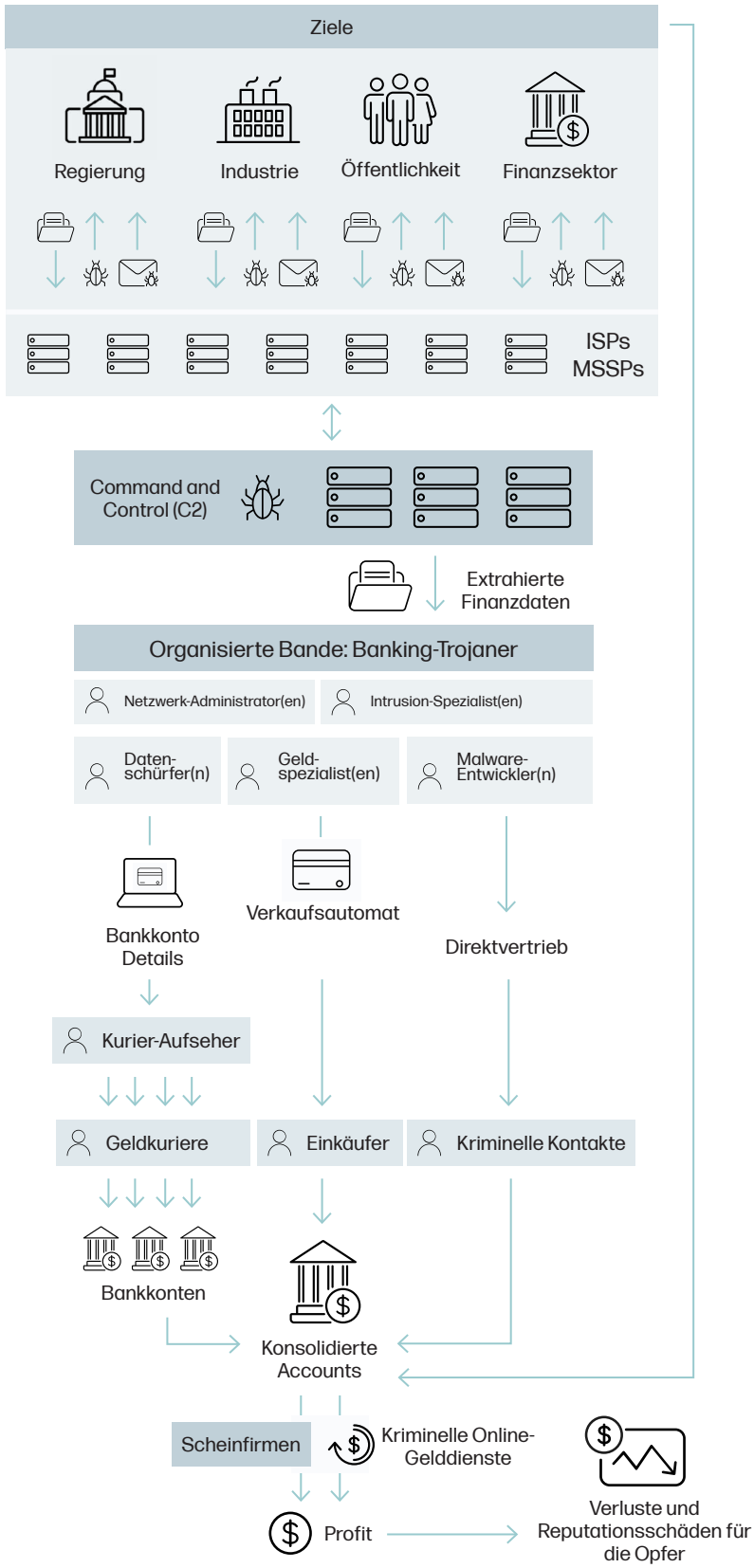
ZeuS kostete 8.000 Dollar,[6] aber ab dem Jahr 2009 musste es mit dem nur 1.000 Dollar teuren Banking-Trojaner SpyEye konkurrieren.[7] SpyEye unterbot ZeuS nicht nur preislich, sondern verfügte auch über eine "Kill ZeuS"-Funktion, mit der der Konkurrent deinstalliert werden konnte, wenn er auf einem infizierten PC vorhanden war.[8]

Die Projekte ZeuS und SpyEye wurden später zusammengelegt,[9] aber die Veröffentlichung des ZeuS-Quellcodes führte bald darauf zu einer starken Zunahme der Cyberkriminalität und zu einer Vielzahl von ZeuS-Varianten, die bei Angriffen eingesetzt wurden, darunter die Banking-Trojaner ICE IX, Citadel und KINS.[10 11 12]

ZeuS	8,000 $
SpyEye incl. "kill ZeuS" feature	1,000 $



Eine geschlossene Gruppe beim Einsatz von Bankentrojanern. Auf der Grundlage von Untersuchungen des britischen National Cyber Security Centre (NCSC) über organisierte Verbrechergruppen und das Ökosystem der Cyberkriminalität zeigt das Diagramm die Beziehungen zwischen den Rollen, der Infrastruktur, den Waren und den Dienstleistungen, die an einem Malware-Unternehmung beteiligt sind.[13]



Neue Monetarisierungsmethoden treiben den Aufstieg von Ransomware voran

Als die Sicherheitsexperten der Strafverfolgungsbehörden und Banken die Oberhand gewannen, indem sie den Cyberkriminellen oftmmals die Kontrolle über Botnetze entrissen, waren gerade Kryptowährungen wie Bitcoin und Monero im Aufwind. Diese Währungen boten Cyberkriminellen eine neue, schwer zu verfolgende Möglichkeit, Angriffe zu finanzieren, bei denen die Vernichtung entwendeter Daten drohte, wenn kein Lösegeld gezahlt wurde.

In dieser Wachstumsphase für destruktive Angriffe verstärkten Cyberkriminelle auch ihre Zusammenarbeit untereinander und bauten ein Ökosystem aus gegenseitiger Unterstützung auf, in dem Personen mit unterschiedlichen illegalen Fähigkeiten spezialisierte Produkte und Dienstleistungen verkauften. Mit anderen Worten: Die Cyberkriminellen begannen, Malware als Service (MaaS) anzubieten.

KEY FACTS

Die Bedrohungsakteure verlagerten sich von Betrug auf Datendiebstahl und destruktive Angriffe.

Die Cyberkriminellen begannen zur Vereinfachung ihrer Angriffe für die Durchführung digitale “As-a-Service”-Modelle zu nutzen.

Ransomware entwickelte sich zur ihrer bevorzugten Methode der Monetarisierung.

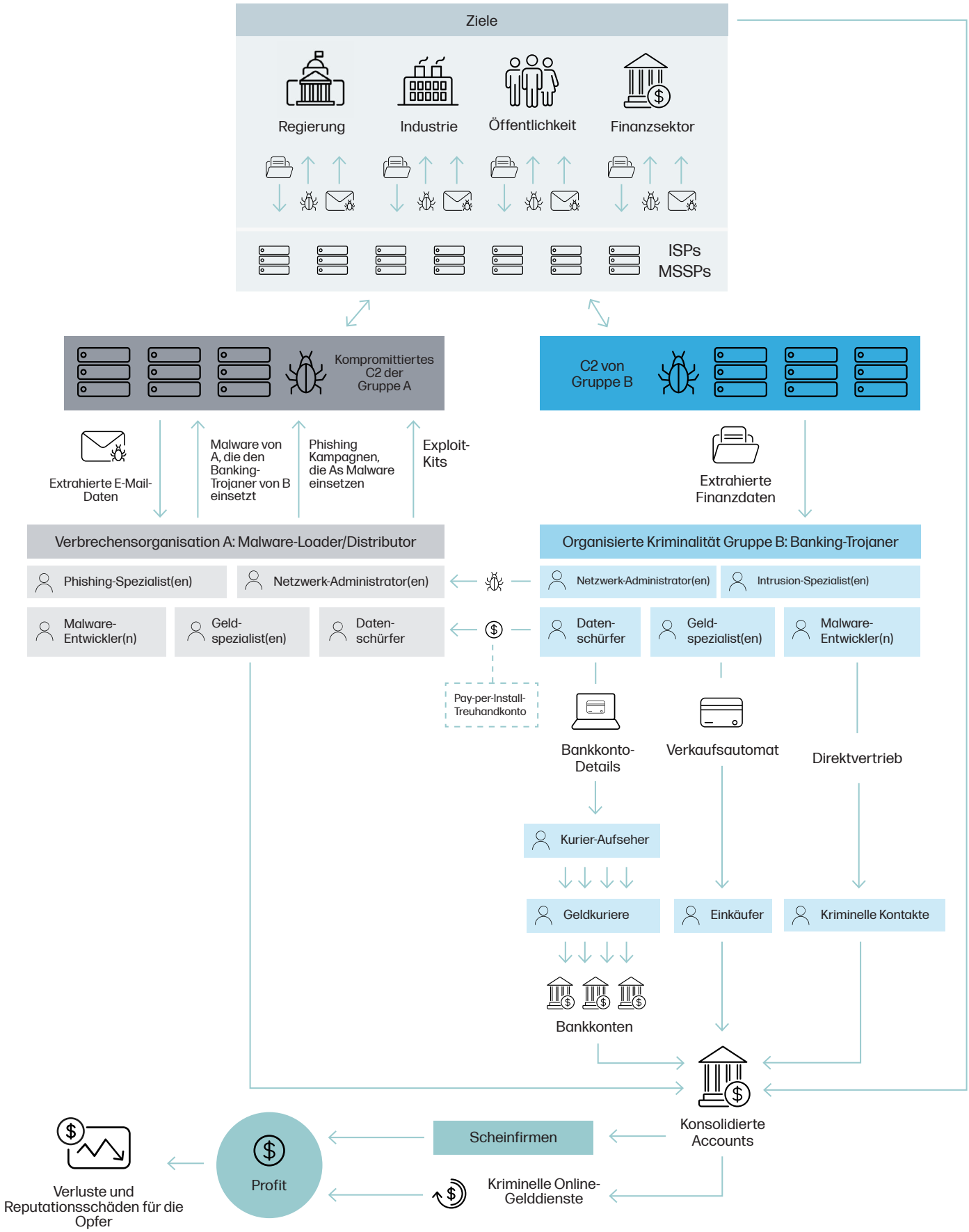
IM FOCUS

Ransomware nimmt zu

Anfangs setzten Ransomware-Varianten wie CryptoLocker auf opportunistische Angriffe, indem sie auf Systeme abzielten, die bereits mit der ZeuS-Variante Gameover ZeuS infiziert waren. Die Angreifer forderten ein Lösegeld in Höhe von 700 US-Dollar oder den Gegenwert in Bitcoin, um die Daten eines infizierten Rechners zu entschlüsseln.[14] Angriffe wie WannaCry und NotPetya trieben diese Methode auf die Spitze, indem sie zerstörerische Methoden einsetzten, um kritische Infrastrukturen lahmzulegen.[15] [16]

CryptoLocker, eine Ransomware-Variante, die über das Gameover-ZeuS-Botnet Verbreitung findet

Ein Diagramm, das die an einer Malware-Verbreitung beteiligten Unternehmen, Waren und Dienstleistungen aufzeigt. Der Malware-Distributor A überlässt Organisation B das Schadprogramm über eine "Access-as-a-Service"-Vereinbarung.[13]



Unternehmen geraten ins Visier der gierigen Kriminellen

Seit 2018 hat sich die Cyberkriminalität weiter in Richtung Service- und Plattform-Geschäftsmodelle verlagert, wobei Bedrohungsakteure komplexe Lieferketten anzapfen, um Angriffe mit speziellen "Plug-and-Play"-Komponenten zu starten.

Außerdem sind die Verbrecher organisierter und gezielter geworden. Sie nehmen sich viel mehr Zeit, um die Infrastruktur eines Ziels zu verstehen und so ihre Wirkung zu maximieren – sei es, um ein höheres Lösegeld zu erpressen oder um einen kritischen Teil der Infrastruktur außer Betrieb zu setzen.

"Im letzten Jahrhundert verlagerte sich die Wirtschaft von Einzelhändlern zur Massenproduktion, zu Dienstleistungsmodellen und zu Plattformen wie Amazon", sagt Dr. Mike McGuire, Senior Lecturer in Kriminologie an der University of Surrey, UK. "Das Cyberkriminalitäts-Business hat dies in weniger als 25 Jahren geschafft."

KEY FACTS

Cyberkriminelle bieten spezialisierte Dienste in komplexen Lieferketten an.

Kampagnen können mit "Plug-and-Play"-Diensten und -Lösungen schnell gestartet werden.

Unternehmen werden ins Visier genommen, um die Wirkung zu maximieren und das Lösegeld zu erhöhen.

IM FOCUS

Ransomware-Rollenprofile

Ransomware ist heute die bevorzugte Methode zur Monetarisierung von Cyberkriminalität, wobei die Kriminellen professionell und mit einem hohen Maß an direkter und indirekter Kollaboration arbeiten. Sie lassen sich im Allgemeinen in die folgenden Spezialrollen einteilen:

DISTRIBUTOR

Diejenigen, die für die Verbreitung von Malware verantwortlich sind, zum Beispiel über E-Mail oder Exploit-Kits.

ACCESS-BROKER

Personen, die sich unbefugt Zugang verschaffen und diesen an andere Kriminelle verkaufen.

INTRUSION-SPEZIALISTEN

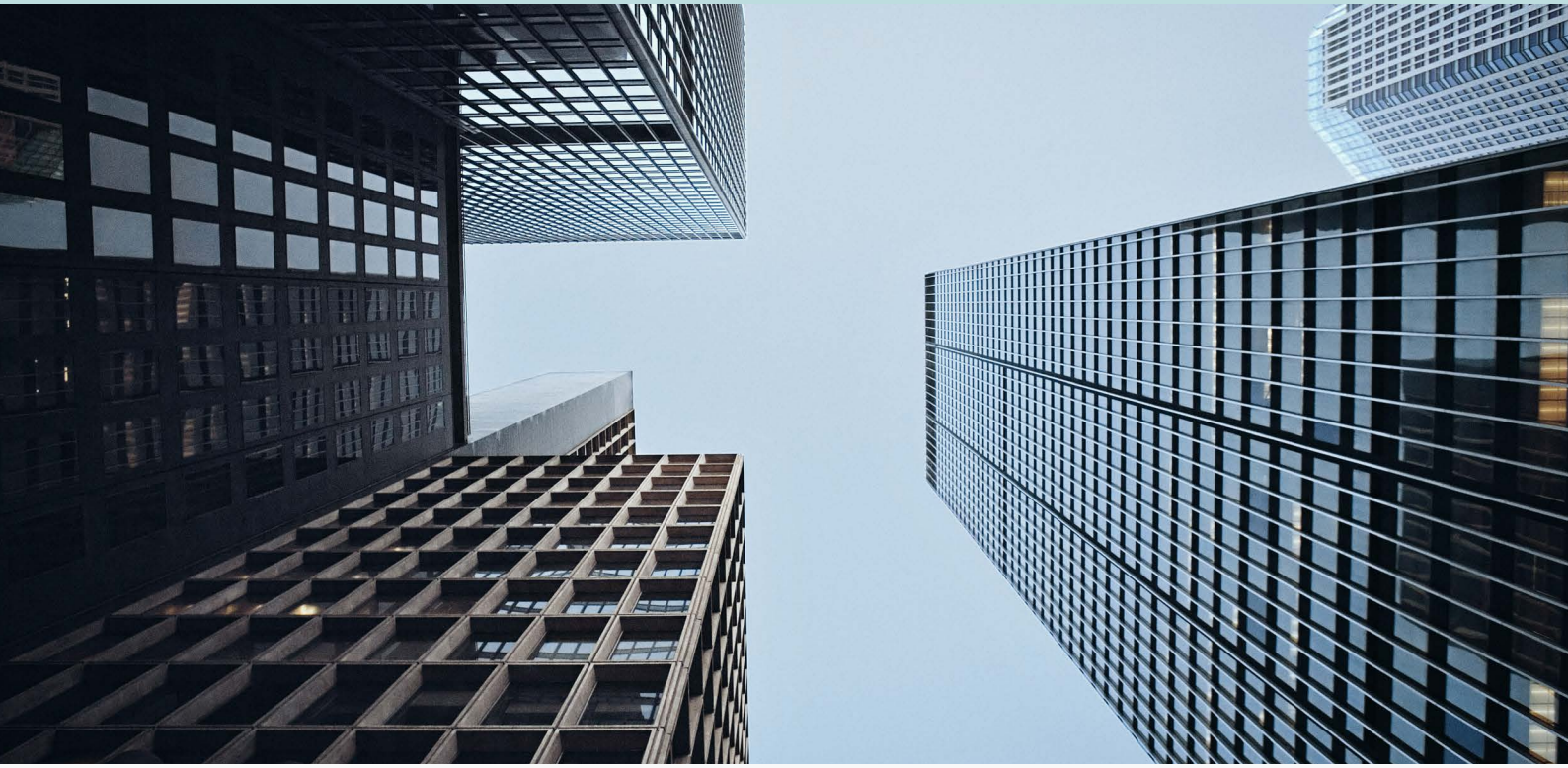
Fachleute für Penetrationstests, auch bekannt als Red Teaming. Sie sind für die Identifizierung und den Diebstahl wertvoller Daten in einem Netzwerk verantwortlich und dehnen das Eindringen auf Punkte aus, an denen Ransomware eingesetzt werden kann, um maximalen Schaden anzurichten.

MONETIZER

Bedrohungsakteure, die sich auf die Abwicklung und Auszahlung von Lösegeld spezialisiert haben.

Abschnitt 02

Zusammenarbeit bei der Cyberkriminalität – Der Einstieg in den heutigen Cybercrime-Komplex



Wenn man die Geschichte der Internetkriminalität verfolgt, wird deutlich, dass Angriffe immer raffinierter und schädlicher werden, wenn Bedrohungsakteure ihr Wissen und ihre Ressourcen zusammenlegen. Eine wichtige Voraussetzung dafür ist der sich ausdifferenzierende Markt in Foren und Chatrooms, die vertrauenswürdige Interaktionen fördern und Unehrlichkeit bestrafen.

Wir haben uns eingehend mit dem Dark Web und Hackerforen befasst, um zu verstehen, wie diese Orte funktionieren und wie Cyberkriminelle sie nutzen, um Angriffe zu kaufen, zu verkaufen und zu diskutieren. Zu diesem Zweck hat Forensic Pathways mit Hilfe automatischer Crawler, die Inhalte im Tor-Netzwerk überwachen, Listen von Dark-Web-Marktplätzen gesammelt. Mit über 35 Millionen indizierten URLs fanden sie rund 33.000 aktive Websites, darunter 5.502 Foren und 6.529 Marktplätze.

KEY FACTS

- Zugang und Kontrolle sind das A und O des Spiels.
- Die Kommodifizierung senkt die Einstiegshürden.
- Die Ironie der Ehre unter Dieben – Warum Reputation im Dark Web zählt.
- Cyber-Oasen für die Rekrutierung und Zusammenarbeit.

Hier sind vier wichtige Erkenntnisse, die Unternehmen beachten sollten:

1. ZUGANG UND KONTROLLE SIND DAS A UND O DES SPIELS

Jedes Eindringen erfordert einen Eintrittspunkt in das Netzwerk des Opfers, was den Zugang und die Kontrolle zum Heiligen Gral der Cyberkriminalität macht. Social Engineering ist einer der beliebtesten Wege in ein System. Im ersten Quartal 2022 wurden 69 % der von HP Wolf Security isolierten Malware per E-Mail verschickt - in Nachrichten, die als harmlos aussehende Geschäftsdokumente getarnt waren.[17]

Ein weiterer Weg führt über gestohlene Benutzernamen und Kennwörter aus dem Dark Web selbst: Unsere Untersuchungen ergaben, dass dort die durchschnittlichen Kosten für Anmeldeinformationen via Remote Desktop Protocol 5 US-Dollar betragen. Eine Website, die Informationen sammelt, die bei Datenschutzverletzungen in Unternehmen verloren gegangen sind, hat nicht weniger als 11 Milliarden Anmeldeinformationen.[2]

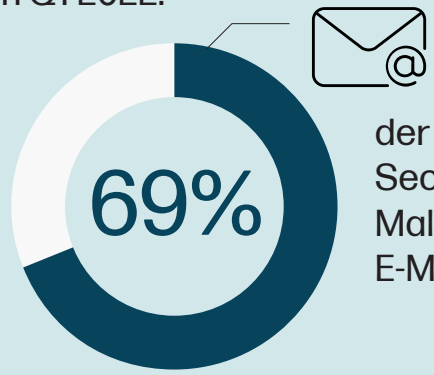
Eine weitere Methode ist das Ausnutzen von Sicherheitslücken und Schwachstellen innerhalb der Software. Unsere Nachforschungen ergaben 130 solcher Schwachstellen, die im Dark Web diskutiert werden, wobei der Schwerpunkt auf den schwerwiegenden, aber einfach auszuführenden Schwachstellen liegt.

Öffentlich bekannt gegebene Schwachstellen werden mit einer CVE-Kennung (Common Vulnerabilities and Exposures) versehen, was bedeutet, dass sie in der branchenweiten Datenbank für Schwachstellen und Gefährdungen (Common Vulnerabilities and Exposures Database) erfasst sind.[18] Im so genannten Common Vulnerability Scoring System werden die CVEs nach ihrem Schweregrad mit 10 Punkten bewertet. Wir fanden heraus, dass der durchschnittliche Schweregrad, der im Dark Web diskutiert wurde, bei 7,4 lag.

Die beliebtesten Ziele waren unterschiedliche Versionen des Windows-Betriebssystems, Microsoft Office, Web-Content-Management-Systeme, Web- und Mail-Server. Bedrohungsakteure konzentrieren sich auf Schwachstellen, die es ihnen ermöglichen, einen ersten Zugang zu Netzwerken und dann die Kontrolle über Systeme zu erlangen.

Selbst die von den Herstellern herausgegebenen Patches zur Behebung von Sicherheitslücken können den Kriminellen helfen. “Anstatt Ressourcen in die Suche nach neuen Schwachstellen zu investieren, halten einige Cyberkriminelle ein wachsames Auge auf neue Hersteller-Patches, um die Schwachstelle durch Reverse Engineering zu verstehen und einen Exploit zu entwickeln. Sie wissen, dass viele Unternehmen den Patch nur langsam einspielen werden”, sagt Dr. Ian Pratt, Global Head of Security for Personal Systems bei HP.

In Q1 2022:



der von HP Wolf Security isolierten Malware wurde per E-Mail versendet.[17]

Eine Website, die bei Datenschutzverletzungen in Unternehmen verloren gegangene Informationen sammelt, hat nicht weniger als

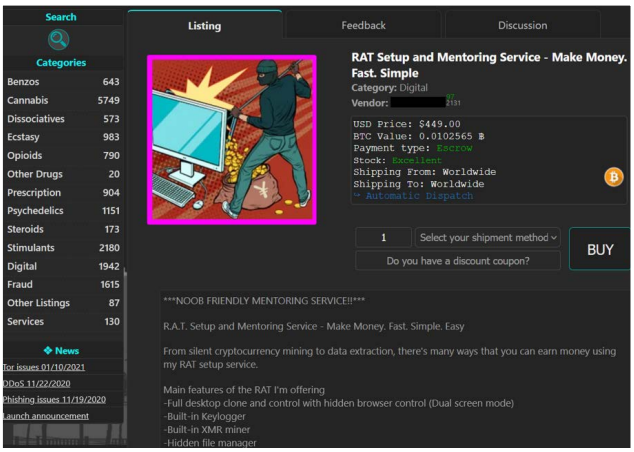
11 Milliarden

Zugangsdaten.[2]

2. KOMMODIFIZIERUNG SENKT DIE EINSTIEGSHÜRDEN

Da Exploits und Malware inzwischen so billig sind, ergeben sich neue Möglichkeiten, Geld zu verdienen: Cyberkriminelle können jetzt die benötigte Angriffssoftware mieten und die Ransomware-Beute mit dem Malware-Anbieter teilen, indem sie ihm eine Provision zahlen. Malware-Autoren differenzieren ihr Produktangebot sogar, indem sie den Nutzern Zugang zu Beratungsdiensten und detaillierten "Playbooks" geben, in denen alles Wissenswerte erklärt wird.

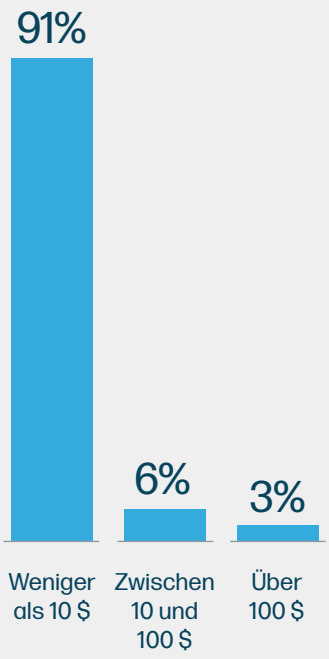
Diese Entwicklung zeigt, dass viele Cyberkriminelle nicht mehr nur Malware-Tools verkaufen, sondern ihr Fachwissen und ihre Fähigkeiten in einer neuen, dienstleistungsorientierten Wirtschaft vermarkten.



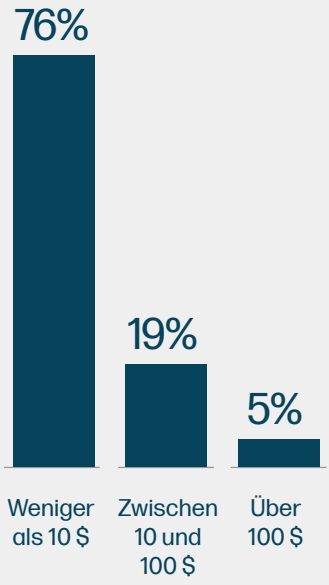
Zum Verkauf stehender Malware-Mentoring-Service

Die niedrigen Kosten der Cyberkriminalität

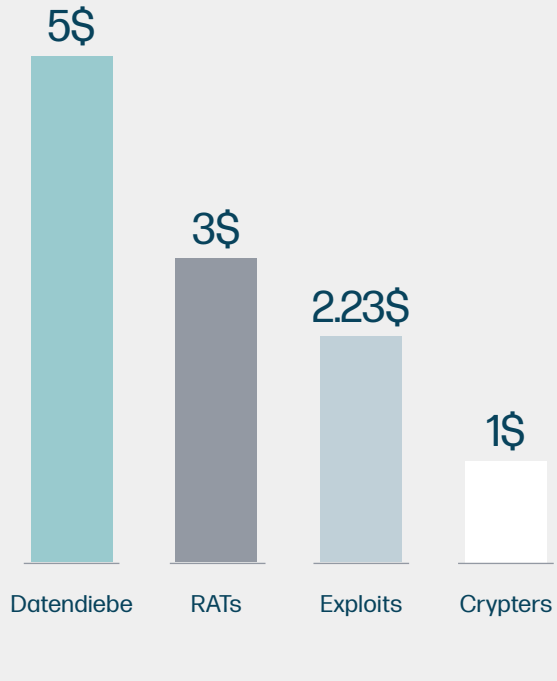
Von 174 im Dark Web beworbenen Exploits kosten:



Preise aus 1.653 Malware-Anzeigen:



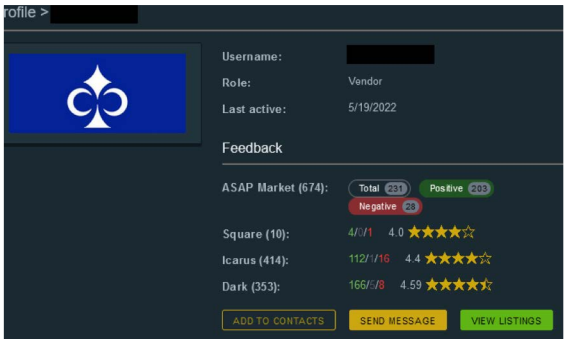
Durchschnittspreis von Malware auf cyberkriminellen Marktplätzen



3. DIE IRONIE DER EHRE UNTER DIEBEN – WARUM REPUTATION IM DARK WEB ZÄHLT

Vertrauen ist für cyberkriminelle Marktplätze unverzichtbar. Deshalb haben sie ausgeklügelte Mechanismen entwickelt, um einen fairen Umgang zu fördern – wie z. B. Reputationsbewertungen von Verkäufern und Käufern sowie Kundenrezensionen.

Da die durchschnittliche Lebensdauer einer Website im anonymen Tor-Netzwerk nur 55 Tage beträgt, haben die Marktplätze Möglichkeiten entwickelt, das Feedback der Verkäufer zu verfolgen, damit es nicht verloren geht, wenn ein Markt geschlossen oder von den Strafverfolgungsbehörden abgeschaltet wird.



Ein Marktplatz mit Bewertungen von Verkäufern auf anderen Märkten

4. CYBER-OASEN FÜR DIE REKRUTIERUNG UND ZUSAMMENARBEIT

Die Möglichkeit, problemlos mit potenziellen Kunden, Partnern und Mitarbeitern in Kontakt zu treten, ist ein wichtiger Bestandteil des Cybercrime-Ökosystems. Foren, spezialisierte Chatgruppen und geschlossene verschlüsselte Netzwerke sind Knotenpunkte, an denen Cyberkriminelle Kontakte knüpfen und Partner anwerben können.

"Das Dark Web ist die cyberkriminelle Vorderseite eines Hauses mit hochmodernem Kundenservice, bei dem Funktionen wie Treuhandzahlungen die Verkäufer in einem überfüllten Markt hervorheben", sagt McGuire.

"Dahinter verbirgt sich jedoch ein verdecktes 'unsichtbares Netz', in dem eine Handvoll mächtiger Gruppen von oben die Fäden zieht und multinationale Cyber-Syndikate leitet, die Informationen austauschen, rekrutieren und zusammenarbeiten, um ihren Ertrag zu maximieren oder sorgfältig ausgewählte Ziele zu stören."

Ergebnisse der Dark Web-Studie zum Reputationsmanagement

100%

der cyberkriminellen Marktplätze verfügen über Anbieter-Feedback-Bewertungen.

77% der cyberkriminellen Marktplätze verlangen einen "Vendor Bond" – eine Verkaufslizenz – die bis zu 3.000 US-Dollar kosten kann.

92% der cyberkriminellen Marktplätze bieten Streitbeilegungsdienste durch Drittanbieter an.

85%

verwenden Treuhandzahlungen, bei denen der Verkäufer das Geld erst erhält, wenn der Käufer das vereinbarte Produkt oder die Dienstleistung erhalten hat.

Abschnitt 03

Horizontscanning – Wie könnte sich die Cyberkriminalität in den nächsten 5 bis 10 Jahren

Vor dem Hintergrund zunehmender Kollaboration, Spezialisierung und Professionalisierung stellt sich nun die Frage, wie sich die Bedrohungslage in Zukunft entwickeln wird. Im Rahmen eines Horizontscannings haben wir vier Schlüsselerwartungen identifiziert, die IT-Sicherheitsexperten beachten sollten.

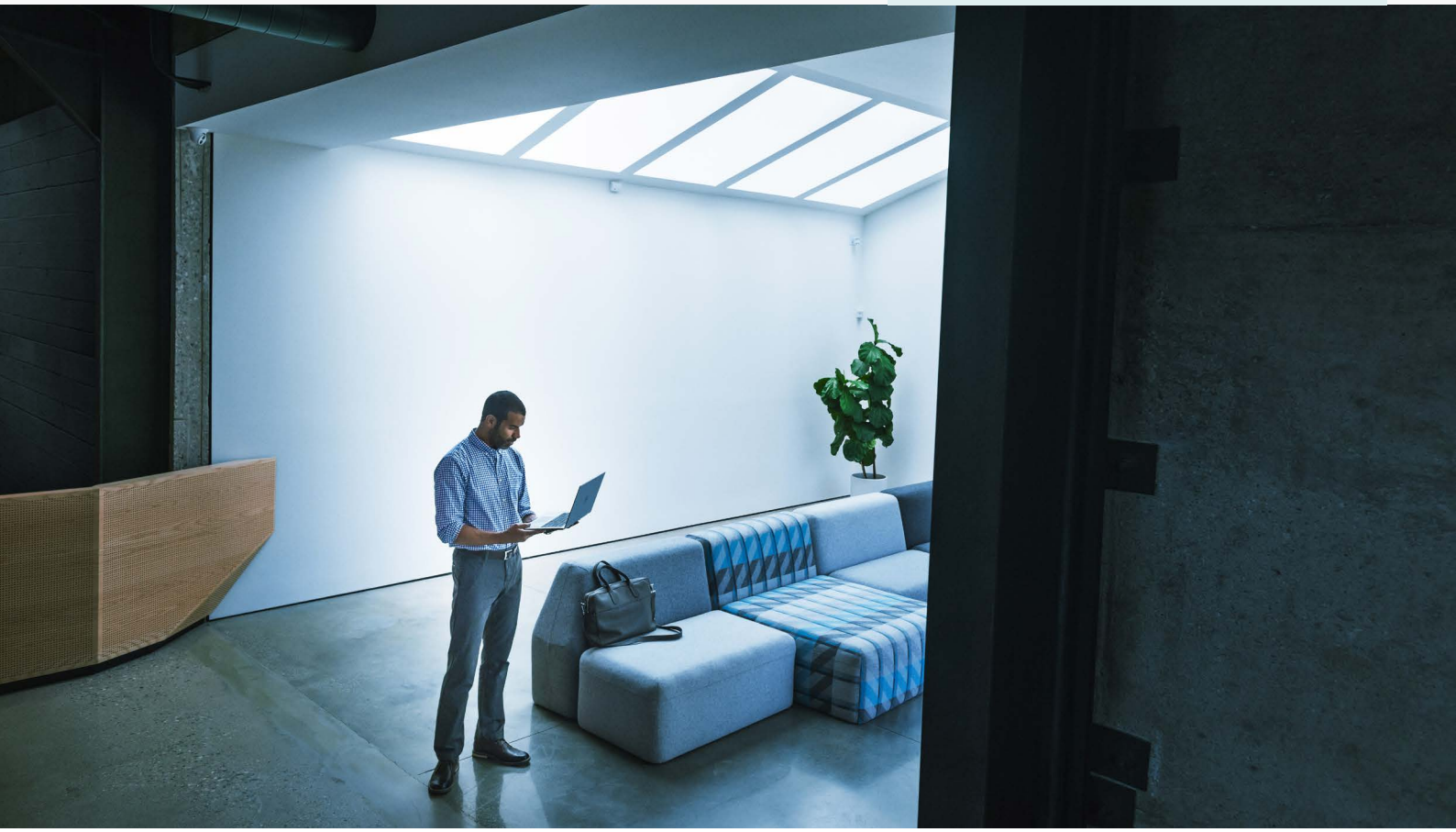
KEY FACTS

Zerstörerische Angriffe durch vorenthaltene Datenwerden noch mehr Schaden anrichten.

Zunehmende Professionalisierung führt zu mehr gezielteren Angriffen.

Aufstrebende Technologien werden sowohl Waffe als auch Schutzschild sein.

Angreifer konzentrieren sich auf Effizienzsteigerungen, um ihre Investitionsrendite zu erhöhen.



1. ZERSTÖRERISCHE ANGRIFFE DURCH VORENTHALTENE DATENWERDEN NOCH MEHR SCHADEN ANRICHTEN

Da Unternehmen zunehmend auf hybrides Arbeiten und digitale Transformation setzen, werden Angreifer die so entstehende immer größer werdende Angriffsfläche wahrscheinlich nutzen. Es ist zu erwarten, dass Erpressungsangriffe mit der Drohung einer Datenzerstörung gegen Branchen eingesetzt werden, die in zeitkritischer Weise auf IoT-Geräte und -Daten angewiesen sind.

Wir sehen auch ein Wiederaufleben zerstörerischer Angriffe auf kritische Infrastrukturen, wie die Wiper-Angriffe Ende 2021 und 2022, die in die Fußstapfen von Shamoon (2012) und Michelangelo (1991) treten – mit Malware, die Daten löscht und Systeme deaktiviert, ohne ein Lösegeld zu verlangen.[19] [20]

2. ZUNEHMENDE PROFESSIONALISIERUNG FÜHRT ZU MEHR GEZIELTEREN ANGRIFFEN

Die Techniken der Cyberkriminalität haben sich in den letzten zehn Jahren denen der staatlich organisierten Hackergruppen von Advanced Persistent Threat (APT), die beispielsweise von Nordkorea aus operieren, angenähert.[21] Diese zeichnen sich durch von Menschen durchgeführte Angriffe aus, die sich ein tiefes Verständnis der Netzwerke der Opfer zunutze machen, und unsere Untersuchungen deuten darauf hin, dass dieses Verwischen der Grenzen weitergehen wird.

Laut McGuire ist Nordkorea führend bei der Nutzung von Cyberkriminalität zur Umgehung von Finanzsanktionen, indem es über seine Lazarus-Hackergruppe in Cyberkriminalität investiert. “Nordkorea hat zweifellos einen Weg aufgezeigt, wie verarmte Länder nicht nur ihre Wirtschaft ankurbeln, sondern auch Sanktionen umgehen können. Das Tor steht nun wirklich offen und das ist eine entscheidende Veränderung der letzten vier Jahre”, sagt McGuire.

3. AUFSTREBENDE TECHNOLOGIEN WERDEN SOWOHL WAFFE ALS AUCH SCHUTZSCHILD SEIN

Es wird erwartet, dass Cyberkriminelle auch Angriffe entwickeln, die sich neue und noch in Entwickelung befindliche Technologien zunutze machen. Dazu könnte eine Verlagerung hin zu Angriffen auf die Datenintegrität gehören, die durch künstliche Intelligenz (KI) angetrieben werden, z. B. wenn Angreifer Organisationen schädigen, indem sie mit Deepfakes gefälschte Nachrichten verbreiten oder KI-Trainingsdaten manipulieren. Dies unterstreicht die Notwendigkeit für Unternehmen, robuste Prüfmechanismen einzuführen, die nicht verändert werden können.

Neue Plattformen wie Web3 könnten ihren Nutzern ein neues Maß an Kontrolle über persönliche Daten bieten. Für Cyberkriminelle könnte dies allerdings neue Möglichkeiten zur Schaffung von Reputationssystemen bedeuten, die die Cyberkriminalität unterstützen und die Zusammenarbeit der Verbrecher untereinander verbessern, indem sie ihre Reputation einfacher über mehrere Marktplätze und Foren hinweg übertragen können.

Ein weiteres Risiko, vor dem man sich in Acht nehmen muss, ist eine mögliche Ausweitung des "Cloud Cracking", bei dem Hacker s in der Cloud verteilte Rechenleistung nutzen, um Brute-Force-Angriffe zu beschleunigen. Sollte dies jemals auf Quantencomputer ausgedehnt werden, könnten die Folgen für die Cybersicherheit katastrophal sein, da diese ultraschnellen Computer dazu verwendet werden könnten, die klassischen kryptografischen Algorithmen zu brechen, die heute den elektronischen Handel, das Bankwesen und die Kommunikation schützen. [22]

4. ANGREIFER KONZENTRIEREN SICH AUF EFFIZIENZSTEIGERUNGEN, UM IHRE INVESTITIONSRENDITE ZU ERHÖHEN

Viele der Schwachstellen, über die Angreifer im Dark Web diskutierten, waren bereits mehrere Jahre alt – und die drei empfindlichsten Angriffsflächen, die HP Wolf Security Anfang 2022 isolierte, waren mindestens vier Jahre alt.[17] Wenn das Zeitfenster, in dem alte Schwachstellen ausgenutzt werden können, so groß ist, ist die Rentabilität von Investitionen zur Nutzung neuer Schwachstellen gering. Stattdessen werden sich Cyberkriminelle eher darauf konzentrieren, die Geschwindigkeit und Effizienz ihrer Angriffe zu erhöhen.

So werden Angreifer in Zukunft wahrscheinlich KI- und maschinelle Learning-Technologie einsetzen, um gezielte Spearphishing-Angriffe in großem Maßstab zu ermöglichen. Angreifer könnten offensive Tools einsetzen, die KI-Funktionen nutzen, um Phishing-E-Mails auf wichtige Personen in einem Unternehmen zuzuschneiden und ihre Aktivitäten nach dem Eindringen in ein Netzwerk zu beschleunigen.

Abschnitt 04

Grundlagen kennen, Resilienz planen, zusammen arbeiten, um das Risiko zu verringern – So steigen Ihre Chancen, das Spiel zu gewinnen

Wie also sollen Organisationen, Unternehmen und Regierungen versuchen, die Möglichkeiten für Internetkriminalität zu verringern? Unser Expertengremium kam zu dem Schluss, dass die Widerstandsfähigkeit gegenüber Cyberkriminalität auf drei wichtige Arten verbessert werden kann.

KEY FACTS

Beherrschen Sie die Grundlagen, um die Chancen von Cyberkriminellen zu verringern

Konzentration auf das Gewinnen des Spiels

Cyberkriminalität ist ein Mannschaftssport: Cybersecurity muss es auch sein

1. Beherrschen Sie die Grundlagen, um die Chancen von Cyberkriminellen zu verringern

BEFOLGEN SIE BEWÄHRTE VERFAHREN

Jedes Unternehmen sollte sicherstellen, dass eine Multifaktor-Authentifizierung eingeführt wird. Kontrollieren Sie genau, welche Software Mitarbeiter installieren dürfen, und sorgen Sie dafür, dass Patches schnell getestet, genehmigt, bereitgestellt und überprüft werden.

REDUZIEREN SIE IHRE ANGRIFFSFLÄCHE

Konzentrieren Sie sich auf die Verringerung des Risikos, das von den wichtigsten Angriffsvektoren wie E-Mail, Webbrowsing und Dateidownloads ausgeht. Investieren Sie in Sicherheitskontrollen, wie z. B. Isolationstechnologien, die das Risiko von ganzen Vektoren eliminieren, aber die Arbeitsabläufe der Mitarbeiter nicht behindern.

PRIORITIZE SELF-HEALING HARDWARE TO BOOST RESILIENCE

In Anbetracht der Tatsache, dass es unweigerlich zu Sicherheitsverletzungen kommt, ist es sinnvoll, widerstandsfähige, selbstheilende Hardware zu verwenden, damit die Wiederherstellung nach einem Angriff so schnell wie möglich erfolgt.

> "CISOs haben eine riesige Liste von Sorgen – je mehr man davon durch eingebaute Sicherheit streichen kann, desto besser. Letztlich ist die größte Schwachstelle der Mensch.
>
> Aus diesem Grund müssen Unternehmen die Sicherheit als ihr ureigenes Aufgabengebiet betrachten. Sie müssen die Technik optimieren und die Widerstandsfähigkeit von der Hardware an aufwärts einbauen, um so ihre Angriffsfläche zu verringern und die Last von einzelnen Mitarbeitenden zu nehmen."
>
> Michael Calce, Vorsitzender des HP Security Advisory Boards und ehemaliger Hacker "MafiaBoy"

2. Konzentration auf das Gewinnen des Spiels

PLANEN SIE FÜR DEN WORST CASE

Fokussieren Sie sich nicht nur auf Ihre Verteidigung, sondern auch auf die Geschäftskontinuität im Falle eines Angriffs. Wenn Sie sich im Voraus darauf vorbereiten und voraussehen, welche Taktiken Angreifer anwenden könnten, können sich Unternehmen schneller erholen.

BEGRENZEN SIE DAS VON IHREM TEAM UND DEN PARTNERN AUSGEHENDE RISIKO

Sie spielen ist nur so stark wie Ihr Team. Unternehmen sollten über Verfahren verfügen, um die Sicherheit von Lieferanten zu überprüfen und ihre Mitarbeitenden über Social Engineering aufzuklären.

SEIEN SIE PROZESSORIENTIERT UND ÜBEN SIE REAKTIONEN

Üben Sie das Verhalten auf Angriffe ein, damit Sie Probleme erkennen, Verbesserungen vornehmen und vorbereiteter sind. “Wir müssen uns von der Überwachung der Statistiken verabschieden und uns mehr darauf konzentrieren, das Spiel zu gewinnen. Man kann ein Team mit außergewöhnlichen Kennzahlen und soliden Spielern haben, aber was zählt, ist: Kann es gewinnen, wenn es darauf ankommt”, so Robert Masse, Mitglied des HP Security Advisory Boards und Partner bei Deloitte.

“For CISOs, this means: can your team detect, prevent, and recover from an attack before it gets serious? Having regular practice games, monitoring performance, strategizing tactics and potential adversarial maneuvers – these are things that can help you beat the odds.”

> “Wenn der Ernstfall eintritt und ein Angreifer Ihre Verteidigungsmaßnahmen durchbricht, dann wollen Sie nicht, dass dies das erste Mal ist, dass Sie einen Notfallplan initiieren.
>
> Wenn Sie sicherstellen, dass alle ihre Rollen kennen und mit den Prozessen vertraut sind, die sie befolgen müssen, können Sie das Schlimmste verhindern.”
>
> Joanna Burkey, HP Chief Information Security Officer

3. Cyberkriminalität ist ein Mannschaftssport: Cybersecurity muss es auch sein

SPRECHEN SIE MIT IHREN KOLLEGEN

Angreifer arbeiten mehr denn je zusammen – das sollten auch die Verteidiger tun. Es wird immer wichtiger, Informationen über Bedrohungen in Echtzeit mit Branchenkollegen auszutauschen. "Sicherheitsgrundlagen können einfache Malware stoppen, aber die gefährlichsten Bedrohungen tauchen nur auf, wenn man den Untergrund durchsucht", sagt Justine Bone, Mitglied des HP Security Advisory Boards. "Auf sich allein gestellt, haben die meisten Unternehmen weder die Zeit noch die Ressourcen für so etwas. Als Branche müssen wir mehr in das Verständnis dieser düsteren Welt investieren und diese Informationen mit unseren Kollegen teilen, damit wir uns besser dagegen verteidigen und sie effektiver stören können."

ZUSAMMENARBEIT MIT DEN SICHERHEITSDIENSTEN DRITTER

Ihr Defensivteam sollte Unabhängige wie Sicherheitsgutachter und Penetrationstests hinzuziehen. Diese können Schwachstellen und kritische Risiken aufzeigen, die angegangen werden müssen.

NUTZUNG VON BEDROHUNGSDATEN UND PROAKTIVES SCANNEN DES HORIZONTS

Die Beobachtung offener Diskussionen in Untergrundforen ist eine Gelegenheit für Netzwerkverteidiger, die Bedrohungen zu verstehen, mit denen ihre Organisationen konfrontiert sind, und ihre Verteidigungsmaßnahmen dahingehend zu justieren. "Es ist wichtig, dass Sie Ihre Bedrohungsszenarien proaktiv verstehen. Wenn man zu sehr nach innen schaut, kann man nicht erkennen, was um die Ecke kommt", sagt Boris Balacheff, Chief Technologist für Sicherheitsforschung bei HP Labs.

"Einer der wichtigsten Gründe zur Hoffnung ist die wachsende Größe und Bereitschaft zum Austausch innerhalb der Cybersicherheits-Community. Ähnlich wie bei den Gegnern sind die Zusammenarbeit und der informative Dialog unerlässlich, um sich gegen die Flut von Angriffen zu wehren.

"Durch proaktives Scannen der Umgebung nach Bedrohungen und den Austausch von Erkenntnissen mit unseren Kollegen können wir gemeinsam eine sicherere und widerstandsfähigere digitale Welt schaffen."

Alex Holland, leitender HP Malware-Analyst

Methodik

HP gab eine unabhängige Studie in Auftrag, die von der Dark-Web-Untersuchungsfirma Forensic Pathways durchgeführt wurde.

Das Unternehmen sammelte Marktplatzeinträge im Dark Web mit Hilfe automatischer Crawler, die Inhalte im Tor-Netzwerk überwachen. Das Tool "Dark Search Engine" verfügt über einen Index, der aus mehr als 35 Millionen URLs mit gesammelten Daten besteht.

Diese gesammelten Daten wurden von den Analysten bei Forensic Pathway untersucht und validiert. Für diesen Bericht wurden etwa 33.000 aktive Websites im Dark Web analysiert, darunter 5.502 Foren und 6.529 Marktplätze. Zwischen Februar und März 2022 identifizierte Forensic Pathways 17 kürzlich aktive Marktplätze für Cyberkriminalität und 16 Hackerforen im Tor-Netzwerk und im Internet, die relevante Einträge enthalten, aus denen der Datensatz besteht.

Über HP Wolf Security

HP Wolf Security* vervollständigt HPs Portfolio an hardwaregestützter Sicherheit und endpunktorientierten Sicherheitsservices, die Unternehmen dabei helfen sollen, PCs, Drucker und Mitarbeitende vor Cyberangriffen zu schützen.

HP Wolf Security bietet umfassenden Endgeräteschutz und Ausfallsicherheit von der Hardware-Ebene über die Software bis hin zu den Services. Erfahren Sie mehr dazu auf hpwolf.com.

*HP Security ist jetzt HP Wolf Security. Die angebotenen Sicherheitsfunktionen variieren je nach Plattform, Details entnehmen Sie bitte dem Produktdatenblatt.

Über Forensic Pathways

Forensic Pathways Ltd. ist spezialisiert auf Threat Intelligence, Cybersicherheitsdienste, Dark Web Monitoring und Social-Media-Untersuchungen.

Im Jahr 2016 begann Forensic Pathways mit dem Scrapping von Daten aus dem Tor-Netzwerk und versteckten Diensten (Dark Web). Mit der "Dark Search Engine" kann das Dark Web sicher durchsucht und auf relevante Inhalte überwacht werden.

Glossary of Key Cybercrime Terms

ADVANCED PERSISTENT THREAT (APT) – in hochgradig fähiger Bedrohungsakteur, der sich unbefugt Zugang zu einem Zielnetzwerk verschafft und über einen langen Zeitraum hinweg unentdeckt bleibt.

BULLETPROOF HOSTING (BPH) – ein Web-Hosting-Anbieter, der das Hosten fast aller Arten von Inhalten, wie z. B. Malware, zulässt und Maßnahmen ergreift, um die Privatsphäre seiner Kunden zu schützen.

DARK WEB – ein Teil des Internets, der nicht von Suchmaschinen indiziert wird.

DDOS (Distributed Denial of Service) – (Distributed Denial of Service) – ein Angriff, der ein System oder einen Dienst unzugänglich macht, indem er es mit Anfragen von vielen Systemen überflutet.

ESCROW SERVICES – eine treuhänderische Vereinbarung, bei der eine dritte Partei Gelder erhält und auszahlt, sobald alle als Teil eineer Transaktion vereinbarten Bedingungen erfüllt sind.

EXPLOIT – Code, Daten oder Befehle, die eine Schwachstelle in einer Anwendung oder einem System ausnutzen, um ein unbeabsichtigtes oder unvorhergesehenes Verhalten hervorzurufen.

EXPLOIT BUILDERS – Tools, mit denen Benutzer einen Exploit ohne Programmierung erstellen können, wodurch die Einstiegshürde für Cyberkriminelle gesenkt wird, sich Zugang zu anfälligen Systemen zu verschaffen.

FULLY UNDETECTABLE (FUD) – bezieht sich auf die Fähigkeit von Malware, sich der Erkennung zu entziehen.

INTERNET OF THINGS (IoT) – in Alltagsgegenstände eingebettete Computer, die Daten über das Internet senden und empfangen können.

MALWARE – Software, die entwickelt wurde, um einen Computer oder ein Netzwerk nachteilig zu beeinflussen, z. B. um Daten zu beschädigen, zu zerstören oder zu stehlen.

MALWARE AS A SERVICE – das Ökosystem von spezialisierten Malware-Produkten und -Dienstleistungen, die von Cyberkriminellen gekauft und verkauft werden.

PACKERS – Tools, die ausführbare Dateien komprimieren, um deren Größe zu verringern. Sie werden häufig zur Verschleierung von Malware eingesetzt.

PHISHING – eine Social-Engineering-Technik, bei der ein Angreifer versucht, ein Opfer dazu zu bringen, vertrauliche Informationen preiszugeben oder seinen Computer per E-Mail mit Malware zu infizieren.

PURPLE TEAMING – eine Methode, bei der ein rotes Team und ein blaues Team (defensive Cybersicherheitsspezialisten) eng zusammenarbeiten, um die Sicherheit einer Organisation zu maximieren.

RANSOMWARE – Malware, die den Zugang zu einem Computersystem verweigert, bis eine Geldsumme gezahlt wird.

REMOTE ACCESS TROJAN (RAT) – Malware, die es einem Angreifer ermöglicht, einen Computer aus der Ferne zu kontrollieren.

RED TEAM – eine Gruppe von offensiven Cybersicherheitsspezialisten, die die Systeme, Prozesse und Mitarbeitende eines Unternehmens auf Sicherheitsrisiken hin überprüfen.

REMOTE DESKTOP PROTOCOL (RDP) – ein Protokoll, das es Benutzern ermöglicht, über ein Netzwerk eine Fernverbindung zu einem anderen Computer herzustellen, den Bildschirm zu sehen und Befehle in das Gerät einzugeben.

SPEAR PHISHING – eine Form des Phishings, die auf bestimmte Personen oder Gruppen innerhalb einer Organisation abzielt.

INFORMATION STEALER – Malware, die vertrauliche Informationen von einem System sammelt, wie z. B. Benutzernamen und Kennwörter.

TOR – Tor, kurz für The Onion Router, ist eine freie und quelloffene Software zur anonymen Kommunikation.

TROJAN – Malware, die als legitime Software getarnt ist.

ZERO DAY – eine noch nicht entdeckte Software-Schwachstelle, die von Angreifern ausgenutzt werden kann, um ein bösartiges Ziel zu erreichen, z. B. unberechtigten Zugang zu einem System zu erhalten.

References

[1] Clarifyi. (2022). *The forensic approach to Threat Intelligence* [Online]. Zu erreichen unter: https://clarifyi.com/

[2] Federal Bureau of Investigation. (2022). *Federal Bureau of Investigation Internet Crime Report 2021* [Online]. Zu lesen unter : https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[3] T. Hunt. (2022). *Have I Been Pwned* [Online]. Zu finden auf: https://haveibeenpwned.com/

[4] Radware. (2022). *IRC (Internet Relay Chat)* [Online]. Zu finden auf: https://www.radware.com/security/ddos-knowledge-center/ddospedia/irc-internet-relay-chat/

[5] Trend Micro. (2015, Aug. 31). *A Brief History of Notable Online Banking Trojans* [Online]. Zu lesen auf: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans

[6] B. Acohido. (2014, Feb. 5). *Lessons from the capture of SpyEye's mastermind* [Online]. Zu lesen auf: https://eu.usatoday.com/story/cybertruth/2014/02/05/lessons-capture-spyeye-mastermind/5182697/

[7] Federal Bureau of Investigation. (2014, Jan. 28). *Botnet Bust: SpyEye Malware Mastermind Pleads Guilty* [Online]. Zu finden auf: https://www.fbi.gov/news/stories/spyeye-malware-mastermind-pleads-guilty

[8] B. Krebs. (2010, Apr. 1). *SpyEye vs. ZeuS Rivalry* [Online]. Zu lesen auf: https://krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/

[9] B. Krebs. (2010, Oct. 24). *SpyEye v. ZeuS Rivalry Ends in Quiet Merger* [Online]. Zu lesen hier: https://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/

[10] D. Fisher. (2011, May 10). *Zeus Source Code Leaked* [Online]. Zu lesen hier: https://threatpost.com/zeus-source-code-leaked-051011/75217/

[11] A. K. Sood, R. J. Enbody, R. Bansal. (2012, Aug. 1). *Inside the ICE IX bot, descendent of Zeus* [Online]. Zu lesen auf: https://www.virusbulletin.com/virusbulletin/2012/08/inside-ice-ix-bot-descendent-zeus

[12] B. Krebs. (2013, Jul. 25). *Haunted by the Ghosts of ZeuS & DNSChanger* [Online]. Zu lesen auf: https://krebsonsecurity.com/2013/07/haunted-by-the-ghosts-of-zeus-dnschanger/

[13] National Cyber Security Centre. (2017, Apr. 9). Cyber crime – understanding the online business model [Online]. Archiv-Version hier: https://www.ncsc.gov.uk/pdfs/news/ncsc-publishes-new-report-criminal-online-activity.pdf

[14] United States Department of Justice. (2014, Jun. 2). *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator* [Online]. Lesbar hier: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[15] BBC News. (2017, May 13). *Massive ransomware infection hits computers in 99 countries* [Online]. Lesbar hier: https://www.bbc.co.uk/news/technology-39901382

[16] MITRE Corporation. (2022, Apr. 25). *NotPetya* [Online]. Zu lesen auf: https://attack.mitre.org/versions/v11/software/S0368/

[17] HP Wolf Security. (2022, May 12). *HP Wolf Security Threat Insights Report Q1 2022* [Online]. Zu finden unter: https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf

[18] MITRE Corporation. (2022). *CVE* [Online]. Erreichbar unter: https://cve.mitre.org/

[19] MITRE Corporation. (2021, Feb. 9). *Shamoon* [Online]. Zu finden unter: https://attack.mitre.org/versions/v11/software/S0140/

[20] Trend Micro. (2017, Mar. 6). *The Michelangelo Virus, 25 Years Later* [Online]. Lesbar auf: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-michelangelo-virus-25-years-later

[21] L. Constantin. (2019, Apr. 10). *Cybercrime groups raise the bar for security by borrowing APT techniques* [Online]. Zu lesen auf: https://www.csoonline.com/article/3387943/cybercrime-groups-raise-the-bar-for-security-teams-by-borrowing-apt-techniques.html

[22] J. Chu. (2016, Mar. 3). *The beginning of the end for encryption schemes?* [Online]. Finden auf: https://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303

Die HP Services unterliegen den geltenden HP Servicebedingungen, die dem Kunden zum Zeitpunkt des Kaufs zur Verfügung gestellt oder angezeigt werden. Der Kunde kann gemäß den geltenden lokalen Gesetzen zusätzliche gesetzliche Rechte haben, die in keiner Weise von den HP Servicebedingungen oder der mit einem HP Produkt gelieferten eingeschränkten HP Garantie berührt werden.

© Copyright 2022 HP Development Company, L.P. Die in diesem Dokument enthaltenen Informationen können ohne vorherige Ankündigung geändert werden. Die einzigen Garantien für HP Produkte und Services sind in den ausdrücklichen Garantieerklärungen enthalten, die diesen Produkten und Services beiliegen. Nichts hierin ist als zusätzliche Garantie auszulegen. HP haftet nicht für technische oder redaktionelle Fehler in diesem Dokument.