Betrüger bestehlen sich gegenseitig

Sicherheitsexperten von Sophos analysierten drei Untergrundforen und deren Schlichtungsräume für Streitigkeiten. Fazit: Wenn zwei Kriminelle sich streiten, freut sich die Verteidigung, die dadurch wertvolle Informationen erhält.



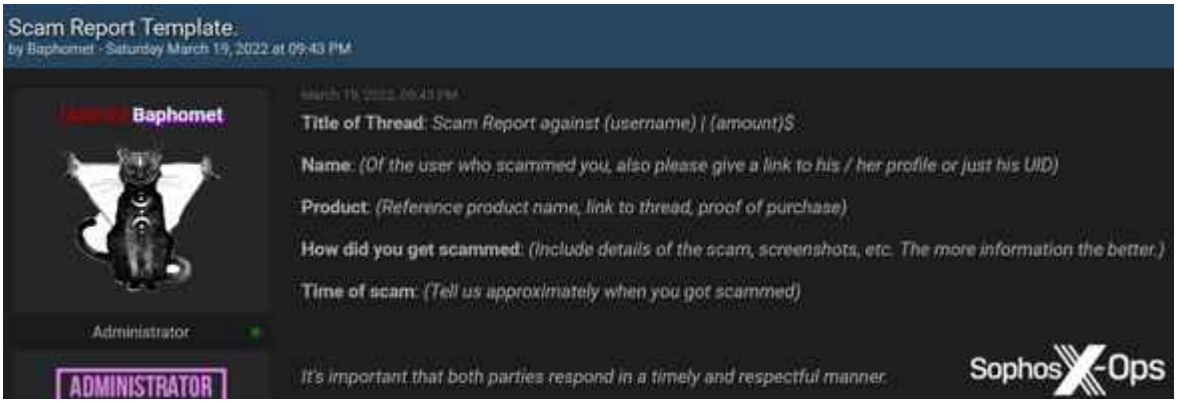
Markt + Trends | IT-Sicherheit

Dass die Schattenwelt der Internetkriminellen genauso arbeitsteilig agiert wie die „richtige“ Wirtschaft, ist seit einigen Jahren bekannt. Sicherheitsforscher von Sophos X-Ops veröffentlichen nun im ersten Teil einer vierteiligen Serie neue Details (siehe ix.de/zey7). So verfügen die untersuchten Untergrundforen Exploit und XSS, zwei russischsprachige Cybercrime-Foren für Access as a Service (AaaS), und die englischsprachige, auf Datenlecks spezialisierte Plattform BreachForums mit Marktplatzfunktion über spezielle Schlichtungsräume zur Beilegung von Streitigkeiten. Dort können Nutzer Betrug, Angriffe und Abzocker melden.

Die „Betrüger betrügen Betrüger“-Masche scheint lukrativ zu sein: In einem Zeitraum von zwölf Monaten analysierte Sophos X-Ops rund 600 Betrugsfälle, bei denen die Bedrohungsakteure

allein in diesen drei Foren mehr als 2,5 Millionen US-Dollar aneinander verloren.

Geld ist den Forschern von Sophos zufolge nicht die einzige Motivation, die die Kriminellen gegeneinander agieren lässt. Auch persönliche Streitigkeiten, Rivalitäten zwischen den Akteuren oder auch der Wunsch, den Ruf des anderen zu beschädigen oder den eigenen zu verbessern, gehören zu den Ursachen.



Im Untergrund wie im echten Leben: Beschwerde führen per Formular. *Sophos*

Die Angriffe gingen über das übliche „Abzocken und Verschwinden“ hinaus. Die Forscher sahen Empfehlungsbetrügereien, vorgetäuschte Datenabflüsse und gefälschte Tools, Phishing, URL-Hijacking, „alt rep“-Betrug (das Verfälschen von Reputationswerten durch Einsatz von „Sockpuppets“, also Fake-Accounts), falsche Bürgen, Erpressung, nachgemachte Konten und Backdoors. Auch konnten die Forscher Fälle beobachten, in denen sich betrogene Bedrohungsakteure wiederum an ihren Betrügern rächten.

Die Sicherheitsforscher fanden überdies Indizien für langfristigen, groß angelegten Betrug in Form von neunzehn Websites, alle von derselben Person oder Gruppierung erstellt, die kriminellen Marktplätzen täuschend ähnlich sehen. Sie fordern von neuen Nutzern eine Aktivierungsgebühr in Höhe von 100 Dollar.

Verteidiger

Theoretisch könnte es der Allgemeinheit völlig gleichgültig sein, wie Kriminelle und Betrüger zueinander stehen oder miteinander umgehen. Aber, erläutert Matt Wixey, Senior Threat Researcher bei Sophos, „da Kriminelle oft viele Beweise vorlegen müssen, wenn sie über die Betrügereien berichten, denen sie selbst zum Opfer gefallen sind, liefern sie eine Fülle von taktischen und strategischen Informationen über ihre Operationen – eine bisher ungenutzte Ressource“. Diese Schlichtungsberichte vermittelten außerdem einen Einblick in die Prioritäten der Angreifer, ihre Rivalitäten und Allianzen, „und, ironischerweise, wie anfällig sie für die gleichen Arten von Täuschung sind, die sie gegen ihre Opfer einsetzen“, so Wixey. (ur@ix.de)

ix.de/zey7

- **The scammers who scam scammers on cybercrime forums: Part 1**
- **Folien des Black-Hat-Vortrags von Sophos**
- **BMI-Papier: Strategie zur Bekämpfung der Schweren und Organisierten Kriminalität**
- **NSA-Empfehlungen für Entwickler zum Absichern der Supply Chain**
- **Projekt Sigstore – Software Signing for Everybody**
- **Konzept von Sigstore**
- **verinice.veo DSMS**
- **Playlist der Vorträge der Black Hat 2022**
- **Aagon Bitlocker-Management**

The scammers who scam scammers on

cybercrime forums: Part 1

A shadowy sub-economy is more than just a curiosity – it's booming business, and also an opportunity for defenders. In the first of a four-part series, we look at the forums involved, and how they …

Die Betrüger, die Betrüger in Cybercrime-Foren betrügen: Teil 1

Eine Schattenwirtschaft ist mehr als nur eine Kuriosität – sie ist ein boomendes Geschäft und auch eine Chance für Verteidiger. Im ersten einer vierteiligen Serie betrachten wir die beteiligten Foren und wie sie mit Betrügern umgehen, die Betrüger betrügen

Geschrieben von Matt Wixey

07. Dezember 2022

Bedrohungsforschung AaaS BreachForums Exploit RaidForums Marktplätze empfohlene Betrug Sophos X-Ops XSS

Auf kriminellen Marktplätzen lauert an jeder Ecke ein Betrug. Bereits 2009 wies Microsoft darauf hin, dass die Untergrundwirtschaft voller Unehrlichkeit sei, und 2017 berichtete Digital Shadows über eine Datenbank von „Rippern" (Betrüger, die Kriminelle betrügen), die von Marktplatzbenutzern erstellt wurde. In unserer jüngsten Berichterstattung über Genesis Market haben wir mindestens eine betrügerische Imitation von Genesis festgestellt, die darauf abzielt, naive Möchtegern-Cyberkriminelle (und möglicherweise unerfahrene Sicherheitsforscher und Journalisten) von ihrem Geld zu trennen.

Aber im Allgemeinen hat das Thema nicht viel Aufmerksamkeit erhalten. Warum sollte es denn auch? Wenn Betrüger Kriminelle ins Visier nehmen, umso besser, oder? Zumindest greifen sie sich gegenseitig an, nicht Organisationen oder die breite Öffentlichkeit.

Wir dachten, dass da noch mehr dahintersteckt, also verbrachten wir ein paar Wochen damit, Betrüger zu untersuchen, die Betrüger in drei prominenten Cybercrime-Foren betrügen – eine Recherche, die unserer Meinung nach noch nie zuvor durchgeführt wurde. Und wir fanden fünf überraschende Dinge.

1. Es ist ein großes Geschäft – eine Subökonomie für sich. In den letzten 12 Monaten haben Cyberkriminelle allein in diesen drei Foren über 2,5 Millionen US-Dollar durch Betrug verloren. Tatsächlich ist es ein so lange bestehendes und prominentes Problem, dass Forenadministratoren spezielle „Schlichtungsräume“ eingerichtet haben, in denen Benutzer Betrug, Angriffe und Ripper melden können.

2. Geld ist nicht das einzige Motiv, und es sind nicht nur niederrangige Bedrohungsakteure beteiligt. Persönliche Probleme, Rivalitäten und der Wunsch, den Ruf zu zerstören (oder manchmal zu verbessern), können alle zu Betrug führen. Und es sind nicht nur kleine Gauner. Wir sahen prominente Bedrohungsakteure, die entweder des Betrugs beschuldigt wurden oder selbst Opfer von Betrug wurden.

3. Die Angriffe gehen über das übliche „Rip-and-Run“ hinaus. Wir sahen Verweis-Nachteile, gefälschte Datenlecks und Tools, Typosquatting, Phishing, „Alt-Rep“-Betrug (die Verwendung von Sockenpuppen, um die Reputationswerte künstlich aufzublähen), gefälschte Bürgen, Erpressung, imitierte Konten und Backdoor-Malware. Wir haben sogar Fälle gefunden, in denen sich Bedrohungsakteure rächen, indem sie die Betrüger betrügen, die sie betrogen haben.

4. Wir haben Beispiele für langfristigen, groß angelegten Betrug gefunden. Eine der größten Überraschungen kam, als wir uns mit dieser nachgeahmten Genesis-Seite befassten. Mit einiger Detektivarbeit entdeckten wir neunzehn weitere Websites, die alle von derselben Person oder Gruppe erstellt wurden, alle kriminelle Marktplätze imitierten und alle darauf abzielten, Benutzer dazu zu verleiten, eine „Aktivierungsgebühr“ von über 100 US-Dollar zu zahlen. Wir wissen nicht genau, wer hinter all diesen Seiten steckt, aber wir haben versuchsweise Links zu einem Drogenhändler entdeckt, der auf mehreren dunklen Websites operiert.

So weit, so *Schadenfreude* – aber die große Frage ist immer noch: wen interessiert das? Warum spielt es eine Rolle, wenn sich Kriminelle gegenseitig angreifen? Hier wird es wirklich faszinierend.

5. Betrugsberichte sind eine reichhaltige und wenig erforschte Informationsquelle. Bedrohungsakteure sind sich bewusst, dass kriminelle Foren überwacht werden, und setzen daher häufig auf gute Betriebssicherheit. Wenn sie selbst Opfer von Verbrechen sind – nun ja, nicht so sehr. Da Forenregeln Beweise für Betrugsvorwürfe verlangen, posten Angreifer, denen Unrecht getan wurde, oft gerne Screenshots von privaten Gesprächen und Quellcode, Identifikatoren, Transaktionen, Chatprotokollen und detaillierte Berichte über Verhandlungen, Verkäufe und Fehlerbehebung.

Diese versteckte Subwirtschaft ist nicht nur eine Kuriosität. Es gibt uns Einblicke in die Forumskultur; wie Bedrohungsakteure kaufen und verkaufen; ihre taktischen und strategischen Prioritäten; ihre Rivalen und Allianzen; ihre Anfälligkeit für Täuschung – und spezifische, diskrete Informationen über sie.

In den nächsten Wochen werden wir die Ergebnisse unserer ausführlichen Untersuchung zu diesem Thema teilen – beginnend mit einem Überblick über die beteiligten Foren, wie sie mit

Betrug umgehen, wer wen betrügt und die Größe der Subwirtschaft.

Sie können sich auch unseren Black-Hat-Vortrag zu dieser Forschung ansehen.

Willkommen im Dschungel

Um unsere Untersuchung einzuleiten, haben wir Betrügereien in zwei der ältesten und bekanntesten russischsprachigen Cybercrime-Foren, Exploit und XSS, untersucht. Wir haben auch Betrügereien von BreachForums, dem Nachfolger von RaidForums, das im April 2022 gestartet wurde, aufgenommen.

Die Foren

Exploit ist relativ exklusiv und ein beliebter Marktplatz für Access-as-a-Service (AaaS)-Angebote , bei denen Initial Access Brokers (IABs) den Zugang zu kompromittierten Netzwerken verkaufen . Aber Bedrohungsakteure kaufen und verkaufen dort auch viele andere illegale Inhalte – Malware, Datenlecks, Infostealer-Protokolle, Anmeldeinformationen und mehr. In der Vergangenheit besuchten Ransomware-Gruppen und -Partner Exploit, obwohl dies nach dem Angriff auf die Colonial Pipeline im Jahr 2021 verdeckter wurde, als sowohl Exploit als auch XSS Ransomware-Diskussionen öffentlich untersagten, um negative Aufmerksamkeit zu vermeiden . Heutzutage wird die Rekrutierung von Ransomware-Affiliates in beiden Foren fortgesetzt, obwohl dies eher unter dem Deckmantel von Euphemismen wie „Pentester“ erfolgt.

XSS, früher bekannt als DaMaGeLaBs, ist ebenfalls gut etabliert, obwohl die Mitgliedschaft weniger exklusiv ist als Exploit. Es hostet auch viele AaaS-Angebote und verschiedene andere Inhalte.

Schließlich ist BreachForums der Nachfolger von RaidForums, einem Marktplatz, der sieben Jahre lang lief, bevor er Anfang

2022 von den Strafverfolgungsbehörden beschlagnahmt wurde . BreachForums ist wie RaidForums ein englischsprachiges Cybercrime-Forum und ein Marktplatz, der sich auf Datenlecks spezialisiert hat, darunter personenbezogene Daten, Kreditkarten, Anmeldeinformationen und Ausweisdokumente.

Alle drei Seiten haben dedizierte Schlichtungsräume – Exploit (mit ungefähr 2500 gemeldeten Betrügereien) und XSS (mit ungefähr 760) haben sie seit Mitte der 2000er Jahre und BreachForums seit ihrer Gründung im April 2022. Andere kriminelle Marktplätze, wie Verified, haben sie Sie auch.

Tatsächlich hat Exploit zwei Räume – einen für offene Ansprüche und einen anderen, der als „Schwarze Liste“ bezeichnet wird und bestätigte Betrugsfälle dokumentiert.

Abbildung 1: Arbitration-Bereich von Exploit

Zusätzlich zu einem speziellen Schlichtungsraum führt XSS auch eine lange „Ripper-Liste“, einen Index von Betrugsseiten.

Abbildung 2: Die Ripper-Liste von XSS

Eine Übersicht über Betrugsstatistiken

Wir haben uns alle Betrugsberichte der letzten 12 Monate angesehen, in denen Geldbeträge angegeben wurden. (Mit BreachForums gingen wir zurück zum ersten aufgezeichneten Betrug, da das Forum noch nicht so lange existiert.)

	Exploit (offene Ansprüche)	**Exploit („Schwarze Liste“)**	**XSS**	**Verletzungsforen**
Ansprüche	211	236	120	21
Gesamtmenge	$1,021,998	$863,324	$509,901	$143,722
Bedeuten	$4,843.54	$3,658	$4,249.18	$6,843.90

Modus	$1000	$500	$150	$500
Median	$600	$500	$500	$200
Bereich	$15 – $160,000	$5 – $150,000	$10 – $160,000	$2 – $134,000

Tabelle 1: Eine Zusammenfassung von 12 Monaten Betrugsmeldungen (alle Beträge in USD)

Dies ist zwar nur eine Momentaufnahme, gibt uns aber einige nützliche Einblicke. Erstens beträgt der durch Betrug verlorene Gesamtbetrag (und denken Sie daran, dass dies nur Betrugsberichte betrifft, in denen bestimmte Beträge erwähnt werden – manche tun dies nicht) 2.538.945 $. Das ist eine beträchtliche Menge, wenn man bedenkt, dass es sich nur um drei Foren handelt.

Zweitens ist Exploit das Schlimmste für Betrug, sowohl in Bezug auf die Anzahl der Berichte als auch auf das Geld, das Betrügern verloren geht. Es hat etwa doppelt so viele Mitglieder wie XSS und kann aufgrund seines guten Rufs auch mehr Betrüger anziehen.

Drittens ist der durchschnittliche als gestohlen gemeldete Betrag in allen drei Foren ähnlich, ebenso wie die Bandbreite – was darauf hindeutet, dass das Ausmaß der Betrügereien unabhängig vom Forum gleich ist.

Opfer haben Betrugsmeldungen für nur 2 US-Dollar eingereicht; Angreifer scheinen genauso empört über den Diebstahl ihres Geldes zu sein wie alle anderen, egal wie hoch der Betrag ist.

Am oberen Ende gehen die Betrügereien auf allen drei Marktplätzen in den sechsstelligen Bereich, obwohl dies die Ausnahmen sind. Viele Betrügereien bringen relativ unbedeutende Beträge ein.

Abbildung 3: Niedrige Schadensummen im XSS-Schlichtungsraum

Abbildung 4: Niedrige Forderungsbeträge im Schlichtungsraum von BreachForums

Abbildung 5: Ein Beispiel für einen größeren Betrugsanspruch auf Exploit (130.000 $). Beachten Sie die vielen Details in diesem Betrugsfall, der Informationen über Verhandlungen und Projekte enthält

Bevor wir uns mit dem Schlichtungsverfahren befassen, lohnt es sich zu untersuchen, warum Betrug so weit verbreitet ist. Bereits 2009 argumentierte Microsoft, dass die illegale Cyberkriminalität keine „kriminelle Utopie des leichten Geldes“ sei, sondern ein „Zitronenmarkt“, auf dem die Anwesenheit von Rippern effektiv eine Steuer auf jede Transaktion einführte.

Auch wenn sich die Zeiten geändert haben und Cyberkriminalität immer mehr zur Ware geworden ist, sind kriminelle Marktplätze immer noch der perfekte Nährboden für Betrüger und Ripper. Es gibt keinen Rückgriff auf die Strafverfolgung; es ist eine (halb) anonyme Kultur, die Privatsphäre betont; Websites sind so exklusiv, dass zumindest ein gewisses Maß an implizitem Vertrauen besteht; Sie werden von Kriminellen bevölkert, die sich wohl kaum als potenzielle Opfer betrachten und daher möglicherweise weniger auf der Hut vor Betrug sind. es ist ein offener Markt ohne Regulierung oder Qualitätssicherung; Transaktionen werden mit Kryptowährungen durchgeführt, die effektiv unauffindbar gemacht werden können; und Sicherheitsvorkehrungen wie Bürgen sind optional (und können, wie wir im nächsten Teil unserer Serie sehen werden, selbst in den Dienst von Betrügereien gestellt werden).

Was unternehmen kriminelle Marktplätze

gegen Betrug?

Die Administratoren krimineller Foren sind sich bewusst, dass Betrug ein Problem darstellt. Zusätzlich zu den Schlichtungsstellen verfügen die meisten Marktplätze über sichtbare Warnungen vor Betrügern und befürworten die Verwendung von Bürgen (manchmal auch als „Zwischenhändler“ oder „Mittelsmänner“ bezeichnet) während des Verkaufs – eine Form der Treuhand.



Abbildung 6: Eine Warnung vor Betrug auf der Titelseite von BreachForums

Andere Foren gehen weiter. Verified zum Beispiel warnt Benutzer ausdrücklich vor gefälschten Links zu seinem Forum und befürwortet die Verwendung eines benutzerdefinierten Plugins, um solche Betrügereien zu erkennen:



Abbildung 7: Betrugswarnung von Verified

In ähnlicher Weise veröffentlicht BreachForums eine Liste aller seiner legitimen Domänen sowie einen monatlichen „Transparenzbericht“, um zu bestätigen, dass die Website und die zugehörige Infrastruktur unter seiner Kontrolle bleiben und nicht kompromittiert wurden (obwohl dies wahrscheinlich auch eine Vorsichtsmaßnahme ist Maßnahme aufgrund dessen, was mit RaidForums passiert ist):



Abbildung 8: Einzelheiten zum monatlichen Transparenzbericht von BreachForums

Aber Schlichtungsstellen sind die Hauptmethode für den Umgang mit Betrug. Der Prozess ist relativ einfach. Benutzer, die einen Betrug melden möchten, müssen einen neuen Thread erstellen, den Benutzer anrufen, der sie angeblich betrogen hat, und so viele Details wie möglich über den Vorfall

angeben. BreachForums stellt hierfür eine Vorlage bereit, während XSS lediglich die erforderlichen Details auflistet.



Abbildung 9: Vorlage für Betrugsberichte von BreachForums



Abbildung 10: Die in XSS-Betrugsberichten erforderlichen Daten: Benutzername, Link zum Profil, Kontaktdaten, Beweise (Chatprotokolle, Screenshots, Brieftaschen, Überweisungen), alle zusätzlichen Informationen

Ein Moderator überprüft dann den Bericht, bittet um weitere Informationen, falls erforderlich, markiert den Angeklagten und gibt ihm eine Frist für die Antwort (normalerweise 24 Stunden, kann aber zwischen 12 und 72 Stunden liegen).



Abbildung 11: Ein Exploit-Moderator gibt einem beschuldigten Betrüger 24 Stunden Zeit, um auf einen Vorwurf zu reagieren

Der Angeklagte kann die Forderung akzeptieren, in diesem Fall leistet er dem Opfer Wiedergutmachung. Das ist selten. Häufiger bestreitet der Angeklagte die Behauptung (in diesem Fall entscheidet der Moderator) oder antwortet überhaupt nicht (in diesem Fall kann er vorübergehend oder dauerhaft aus dem Forum ausgeschlossen werden).



Abbildung 12: Ein umstrittener Anspruch auf XSS in Bezug auf AaaS-Angebote

Bei strittigen Behauptungen kann der Moderator für eine Partei entscheiden oder entscheiden, dass aufgrund fehlender Beweise kein Fall zu beantworten ist. In einigen Fällen erhalten eine oder beide Parteien Verwarnungen oder vorübergehende oder dauerhafte Sperren.



Abbildung 13: Der Administrator von BreachForums schließt einen Betrugsbericht aufgrund fehlender Beweise



Abbildung 14: Ein umstrittener Anspruch auf Exploit bezüglich eines Crypters zur Verwendung mit Remcos

Diese Diskussionen sind manchmal zivil und werden gütlich zur Zufriedenheit beider Parteien beigelegt. Wir haben ein Beispiel notiert, bei dem der Schiedsrichter entschied, dass der Angeklagte 50 % des geforderten Betrags zurückzahlen sollte:



Abbildung 15: Ein Exploit-Moderator gibt dem Angeklagten 24 Stunden Zeit, um 50 % des geforderten Betrags zurückzuzahlen

In einem Fall entschädigte der Administrator von BreachForums sogar ein Betrugsopfer aus eigener Tasche:



Abbildung 16: Der Administrator von BreachForums entschädigt ein Betrugsopfer persönlich mit 200 US-Dollar

Betrugsberichte enden jedoch häufiger in Beleidigungen und Gegenanschuldigungen. In einigen Fällen wurden die mutmaßlichen Opfer später selbst wegen Betrugs gesperrt.



Abbildung 17: Ein Betrugsbericht über Exploit führt dazu, dass der Ankläger den Ankläger des Betrugs beschuldigt

Folgen

Verbote (und in geringerem Maße Verwarnungen) scheinen das häufigste Ergebnis in Schiedsverfahren zu sein, aber BreachForums verfolgt einen etwas anderen Ansatz. Vielleicht, um zukünftige Betrüger abzuschrecken, veröffentlichen die Moderatoren die Registrierungs-E-Mail-Adressen und

Registrierungs- und zuletzt gesehenen IP-Adressen gesperrter Benutzer, wodurch sie teilweise doxiert werden:



Abbildung 18: Ein Beispiel eines gesperrten Benutzers, komplett mit veröffentlichter Registrierungs-E-Mail-Adresse, Registrierung und letzten bekannten IP-Adressen

Wir haben einige Fälle von Serienbetrügern bemerkt, die nach einer Sperrung einfach ein neues Profil mit einer neuen Identität erstellten, eine neue Registrierungsgebühr zahlten und wieder mit dem Betrügen begannen.

Nicht nur kleine Gauner

Wir haben einige Beispiele notiert, an denen prominentere Bedrohungsakteure beteiligt waren. Hier ist zum Beispiel ein merkwürdiger Fall, der nicht so sehr ein Betrug war, sondern einen Benutzer betraf, der im Namen eines Opfers mit der Conti-Ransomware-Gruppe verhandeln wollte:



Abbildung 19: Ein Benutzer erhebt eine Schiedsklage, um zu versuchen, mit der Conti-Gruppe über die Entschlüsselung der Vermögenswerte eines Unternehmens zu verhandeln

Dieser Bericht wurde von Exploit-Moderatoren geschlossen, da er sich auf Ransomware bezog, die angeblich in diesem Forum verboten ist. Interessant ist jedoch, dass der Beschwerdeführer selbst ein Bedrohungsakteur zu sein scheint und dem Exploit-Forum über drei Jahre lang beigetreten war, bevor er den oben genannten Anspruch geltend machte – mit mehreren Beiträgen, in denen er sein Interesse am Kauf von Daten bekundete. Ihre Beziehung zu Contis Opfer in diesem Fall ist nicht klar.



Abbildung 20: Einige der früheren Beiträge des Beschwerdeführers im Exploit-Forum

Ein weiterer Fall betraf „Alan Wake“ (ein Name aus einem Videospiel), der den letzten Wettbewerb auf XSS gesponsert hatte und zuvor von einem Lockbit-Betreiber beschuldigt wurde, der Anführer der Ransomware-Gruppen Conti und BlackBasta zu sein . Ein Benutzer beschuldigte Alan Wake, sein Gehalt nicht gezahlt zu haben, weil er „Verkehr aus Muscheln gemacht“ habe:



Abbildung 21: Der XSS-Betrugsbericht gegen „Alan Wake“

Alan Wake bestritt den Vorwurf, und der Fall wurde vom Administrator geschlossen und der Beschwerdeführer gesperrt – nicht wegen Betrugs, sondern wegen „Beleidigungen, Angriffen, Drohungen usw.“ und „äußerst unangemessenem Verhalten“.

Schließlich wurde All World Cards (ebenfalls ein früherer Sponsor von XSS-Wettbewerben), eine prominente Carding-Gruppe, selbst Opfer eines Betrugs mit einer gefälschten Schwachstelle und verlor 2000 USD.



Abbildung 22: Die Gruppe All World Cards meldet einen Betrug, bei dem sie 2000 Dollar verloren hat

Wenn es eine Erkenntnis aus all dem gibt, dann die, dass kein Benutzer immun ist; Jeder Handel in kriminellen Foren birgt ein inhärentes Betrugsrisiko. Obwohl es sowohl proaktive (Warnungen, Plugins, Garanten) als auch reaktive (Schlichtungsstellen) Maßnahmen gibt, sind Betrüger nicht nur üblich, sondern – nach den von uns gesammelten Daten zu urteilen – oft erfolgreich. Einer der Gründe für ihren Erfolg ist die schiere Vielfalt der Betrügereien, die sie ziehen.

Im zweiten Teil unserer Untersuchung, der nächste Woche um diese Zeit (Mittwoch, 14. Dezember) erscheinen wird, behandeln wir die verschiedenen Arten von Betrug, die wir beobachtet haben.



Managed Security Services: 4 kritische Fragen, die Sie stellen sollten

Die Landschaft der Cybersicherheitsbedrohungen ist unglaublich volatil. Cyberkriminelle gehen immer professioneller vor, spezialisieren sich zunehmend und treten sogar in Konkurrenz zu anderen Grup…

Managed Security Services: 4 kritische Fragen, die Sie stellen sollten

Verfasst von Jörg Schindler

24. November 2022

Die Landschaft der Cybersicherheitsbedrohungen ist unglaublich volatil. Cyberkriminelle gehen immer professioneller vor, spezialisieren sich zunehmend und treten sogar in Konkurrenz zu anderen Gruppierungen. In der Folge sind Unternehmen innerhalb von Monaten, Wochen oder Tagen – manchmal sogar gleichzeitig – nicht nur einmal sondern immer wieder Angriffen ausgesetzt.

Der weltweite Arbeitskräftemangel im Bereich Cybersicherheit verschärft diese Herausforderungen. Weltweit hat sich die Personallücke im Bereich Cybersicherheit im Jahr 2022 nach Angaben der „2022 Cybersecurity Workforce Study by (ISC)²“ um 26,2 % erhöht, mit insgesamt mehr als drei Millionen offenen Stellen. Während einige Regionen besser abschneiden als andere – wie beispielsweise Lateinamerika, das die Lücke um 26,4 % schloss – bergen die verbleibenden Engpässe immer noch nationale Sicherheitsrisiken.

Cyberkriminelle sind immer aktiv, und Sicherheitsteams müssen es auch sein. Viele Organisationen, die nicht über die

erforderlichen Ressourcen verfügen, um selbst immer komplexere Cyberbedrohungen zu erkennen und darauf zu reagieren, entscheiden sich für die Nutzung von Cybersecurity-as-a-Service (CSaaS), um proaktive Abwehrmaßnahmen zu implementieren. Beim CSaaS-Modell setzen Unternehmen externe Spezialisten ein, um kritische Cybersicherheitsanforderungen zu erfüllen, wie z. B. Bedrohungsüberwachung rund um die Uhr. Durch die Auslagerung oder Erweiterung von IT-Teams mit Managed Detection and Response (MDR)-Services als zentrales CSaaS-Angebot können Unternehmen dazu beitragen, Angriffe abzuschwächen, bevor sie auftreten. Jedes Unternehmen, das erwägt, den Sicherheitsbetrieb auszulagern, sollte Sicherheitsdienstpartnern diese vier Fragen stellen:

1.Welche Erfahrung haben sie in der Zusammenarbeit mit anderen Unternehmen in unserer Branche und Region?
Wenn der Anbieter mit anderen Organisationen in ihrer Branche und Region zusammenarbeitet, sollten diese über Erfahrungen aus erster Hand bei der Verteidigung gegen die spezifischen Bedrohungen verfügen, denen sie ausgesetzt sind.

2. Können sie unsere bestehenden Technologien verwalten und unterstützen?
Fragen sie, ob der CaaS-Anbieter auf ihren vorhandenen Sicherheitstechnologien aufbauen kann, oder ob sie das, was sie bereits im Einsatz haben, entfernen und ersetzen müssen. Der ideale Anbieter sollte in der Lage sein, mit den vorhandenen Technologielösungen zu arbeiten.

3. Wie ausgereift ist ihr Verständnis von neu auftretenden Cyberbedrohungen?
Kriminelle entwickeln sich häufig in den Taktiken, Techniken und Verfahren (TTPs) weiter, die sie verwenden, um Angriffe möglichst unbemerkt durchzuführen. Unternehmen sollten sehr sorgfältig darauf achten, dass ein potenzieller Anbieter die entsprechenden Ressourcen vorweisen kann, mit denen er eine qualitativ hochwertige Bedrohungsanalyse sowie schnelle Reaktion gewährleisten kann.

4. Kann die Lösung eines potenziellen Partners mit unserem Unternehmen skalieren und sich mit unseren Anforderungen weiterentwickeln?
Es ist von entscheidender Bedeutung, dass jeder potenzielle Partner in der Lage ist, den individuell wachsenden und sich entwickelnden Anforderungen gerecht zu werden und die Unternehmenssicherheit zusammen mit sich ändernden Anforderungen effektiv zu optimieren.

Mit einem starken CSaaS-Anbieter sind Unternehmen in der Lage, eine vollständig etablierte Sicherheitsstruktur mit proaktiven Abwehrmaßnahmen und 24/7-Unterstützung zur realisieren. Dies gibt Unternehmen die Möglichkeit, ihre IT-Operationen kontinuierlich zu verbessern und Organisationsmodelle zu verfeinern, wodurch sie in einer äußerst volatilen Bedrohungslandschaft nicht nur überleben, sondern auch wachsen können.

Black Hat

Black Hat

Betrüger, die Betrüger betrügen, Hacker, die Hacker hacken: Erkundung einer verborgenen Subökonomie in Foren und Marktplätzen für Cyberkriminalität

Matt Wixey | Leitender technischer Redakteur, Sophos
Angela Gunn | Senior Threat Researcher / Cybersecurity Writer, Sophos

Datum : Mittwoch, 7. Dezember | 15:20-16:00 Uhr (Capital Suite Zimmer 7/12 (Ebene 3))

Format : 40-Minuten-Briefings

Spuren : Menschliche Faktoren, Verteidigung Es ist kein Geheimnis, dass kriminelle Foren und Marktplätze mit schändlichen Aktivitäten vollgestopft sind. Aber hinter all den Initial Access Brokern, gestohlenen Daten und Malware gibt es eine versteckte, blühende Unterkategorie der Kriminalität, die unbemerkt bleibt: Bedrohungsakteure, die es auf andere Bedrohungsakteure abgesehen haben. Diese kannibalischen Kriminellen (wir nennen sie „Metaparasiten“: ein Parasit, dessen Wirt auch ein Parasit ist) sind ein so hartnäckiges und teures Problem, dass es spezielle Forenräume gibt – die Tausende von Posts enthalten und Jahre zurückreichen –, die dafür bestimmt sind, sie auf die schwarze Liste zu setzen und Betrug zu schlichten Beschwerden zwischen Benutzern und das Melden von nachgeahmten „Ripper“-Sites. In diesem Vortrag präsentieren wir eine neuartige Untersuchung über Betrüger, die Betrüger betrügen, und Hacker, die Hacker hacken, auf drei der etabliertesten und bekanntesten kriminellen Marktplätze. Wir untersuchen die Größe dieses schattigen Multi-Millionen-Dollar-Ökosystems; die Beweggründe von Metaparasiten; wie Schiedsverfahren funktionieren; und welchen Einfluss Metaparasiten auf die Kultur und den Betrieb der Marktplätze haben, auf denen sie tätig sind. Anschließend tauchen wir tief in Fallstudien ein und betrachten die Techniken, die Metaparasiten verwenden, von altmodischem „Rip and Run“-Betrug und gefälschten Datenlecks bis hin zu ausgeklügelten Phishing-Kampagnen, Verweisbetrug, Typosquatting und Backdoor-Malware. Unterwegs decken wir einen groß angelegten, koordinierten und lukrativen Betrug auf, an dem ein Netzwerk von 15 gefälschten Marktplätzen beteiligt ist, und Fälle, in denen sich die Bedrohungsakteure rächen und die Betrüger betrügen, die sie betrogen haben. Sie könnten fragen: Wen kümmert es, wenn Kriminelle sich gegenseitig abzocken? Aber Metaparasiten bieten Analysten unbeabsichtigt einen Informationssegen, der es uns ermöglicht, beispiellose Einblicke in Verkäufe, Operationen, Verhandlungen und Identifikatoren zu gewinnen,

die sonst verborgen bleiben würden – sowie in die Marktkultur, unterschiedliche Ebenen der Betriebssicherheit und Anfälligkeit für Täuschung und Sozialtechnik. Unser Vortrag wird auch dazu beitragen, Analysten und allgemein Neugierige davor zu schützen, versehentlich auf einige dieser Betrügereien hereinzufallen, wenn sie kriminelle Marktplätze untersuchen.

Präsentationsmaterial

- Folien hier herunterladen

EU verabschiedet NIS2-Richtlinie – Umsetzung bis 2024

Nach dem EU-Parlament hat auch der EU-Rat der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS2) zugestimmt. Die Mitgliedsstaaten müssen sie bis Herbst 2024 in nationales Recht umsetzen. Sie soll die Resilienz und die Kapazitäten zur Reaktion auf Sicherheitsvorfälle sowohl des öffentlichen als auch des privaten Sektors und der EU als Ganzes weiter verbessern. Die NIS2-Richtlinie steht im Zusammenhang mit zahlreichen gesetzgeberischen Maßnahmen im Bereich IT- und Cybersicherheit.

Ähnlich den Vorgaben der KRITIS-Verordnung werden Unternehmen betroffener Branchen verpflichtet, Risikomanagementmaßnahmen zu ergreifen und Meldepflichten zu beachten. Zu den Branchen zählen unter anderem Energie, Verkehr, Gesundheit und digitale Infrastruktur. Um sicherzustellen, dass nur mittlere und große Unternehmen von den Vorgaben erfasst werden, sieht die Richtlinie Schwellenwerte für ihre Anwendbarkeit vor.

Ziel der Richtlinie ist eine Harmonisierung der einschlägigen Bestimmungen in den einzelnen EU-Staaten durch Mindestvorgaben und Regeln zur wirksameren Zusammenarbeit zwischen den

nationalen Behörden. Unter anderem bei Aspekten der Zusammenarbeit und Kooperation sowie den Anforderungen an das Cybersecurity-Risikomanagement geht die Richtlinie deutlich über die NIS1-Richtlinie hinaus. *Tobias Haar* (ur@ix.de)

Kurz notiert

Aagon veröffentlicht ein Produkt zum **BitLocker-Management.** Es bietet die zentrale Verwaltung des Windows-Bordmittels zur Festplattenverschlüsselung sowie Monitoring- und Reportfunktionen.

Seit Kurzem stehen 102 Vorträge der diesjährigen **Sicherheitskonferenz Black Hat** auf dem YouTube-Channel des Veranstalters zum Nachschauen bereit (siehe ix.de/zey7).

Der **verinice.veo-Datenschutzmanager** steht Interessierten in einer Einzelplatz-Betatestversion zur Verfügung. Mit dem Datenschutzmanagementsystem lassen sich die Vorgaben der DSGVO verwalten und ihre Umsetzung gewährleisten.