SWITCH Security Report zu aktuellen Trends im Bereich IT-Security und Privacy

September/Oktober 2023

I. Dem geschenkten Gaul sieht man besser ins Maul: Phishing mit Wohnwagen- und Wohnmobil-Angeboten

Das Angebot des Inserats auf Gebrauchtfahrzeug-Portalen klingt verlockend: weil es angeblich ausgewandert sei und keinen Bedarf mehr hätte, möchte ein Paar sein älteres gebrauchtes Freizeitgefährt einer bedürftigen Familie schenken oder zu sehr günstigen Konditionen verkaufen. Um die – in des Wortes doppeltem Sinne – Glaubwürdigkeit des Ansinnens zu belegen, gibt die Inserentin sich und ihren Mann als bibelgläubige Christen aus, die es ernst meinten und nicht mit den Gefühlen von Menschen spielen wollten. Was zu gut klingt, um wahr zu sein, ist es auch: Anfangs Oktober warnte die Polizei davor, dass es sich dabei um Lockvogelangebote handelt, mit denen gutgläubige Opfer meist doppelt geschädigt werden:

Zum einen werden sie aufgefordert, ihre Personendaten samt Pass- oder ID-Karten-Kopie zu senden, weil sich das Fahrzeug im Ausland befinde. Die auf diese Weise ergaunerten Daten werden dann später für weitere, von der Polizei nicht näher bezeichnete Delikte verwendet.

Zum anderen informieren die Betrüger im Lauf des weiteren Kaufprozesses die Opfer darüber, dass für den Export des Fahrzeugs Transport- und Zollgebühren anfallen würden. Haben die Opfer überwiesen, brechen die Betrüger den Kontakt ab, und Daten und Geld der Opfer sind

verloren. Im schlimmsten Szenario werden die Passbilder dann auch noch verwendet, um Deep Fakes zu produzieren und zu verbreiten.

Die aktuellen Fälle zeigen, dass solche sogenannten «Impersonation Attacks» vermehrt zu beobachten sind. In einem interessanten nachstehend verlinkten Blogbeitrag hat das Sicherheitsunternehmen UpGuard die unterschiedlichen Formen solcher Attacken übersichtlich aufgelistet und beschrieben, wie sich Userinnen und User vor ihnen schützen können.

Nachzulesen unter:

https://www.cybercrimepolice.ch/de/fall/lockvogel-inserate-mit-wohnmobilen-und-wohnwagen
https://polizei.news/2023/10/11/betrugsmasche-lockvogel-inserate-mit-wohnmobilen-und-wohnwagen
https://www.upguard.com/blog/impersonation-attack#:~:text=An%20impersonation%20attack%20is%20a,giving%20up%20sensitive%20information%2C%20or

II. Urlaubs-Nachlese der kriminellen Art: Raffinierte Angriffe auf Hotels, Reisebüros und Buchungs-Plattformen

Ganz anders und überaus raffiniert läuft seit September eine mehrstufige Angriffswelle gegen Hotels, Reisebüros und Buchungsplattformen. Auch hier ist das Ziel, sensible Daten – in diesem Fall die kompletten Kreditkarten-Daten – zu erbeuten. Wie das Security-Unternehmen «Perception Point» berichtet, gehen die Cyberkriminellen dabei besonders raffiniert und überaus vorsichtig zu Werke, indem sie zunächst selbst eine Buchungsanfrage an ein Hospitality-Unternehmen (Hotel oder Reisebüro) schicken. Auf dessen Antwort hin, senden Sie eine sehr persönlich gestaltete und emotional berührende E-Mail mit einer Zusatzfrage oder einem speziellen Wunsch und einem Link zu einem File Sharing Dienst. Um ihre Glaubwürdigkeit zu unterstreichen, senden sie dazu ein Klartextpasswort, mit dem sich das angegriffene Unternehmen auf dem File Server anmelden und ein kompromittiertes Archiv – und damit eine Spionage- und Datendiebstahlssoftware – herunterladen kann.

Einmal ausgeführt, klicken sich die Cyberkriminellen in die Kundendaten des Opfers und starten den direkten Dialog mit diesen Kunden. Sie werden aufgefordert, nach einem vermeintlichen System-Update weitere notwendige Daten ihrer Kreditkarte zu senden, damit die Buchung bestehen bleiben kann. Der mitgeschickte Link führt auf eine täuschend echt aussehende, jedoch gefakte booking.com-Seite. Wie Perception Point schreibt, sei die Kampagne in ihrer Mehrstufigkeit bereits an sich überdurchschnittlich ausgefeilt angelegt. Dazu käme aber, dass die einzelnen Angriffsstufen auch noch überaus raffiniert und gekonnt ausgeführt seien.

Weit einfacher gelang es offenbar den in Security-Kreisen ebenso bekannten wie gefürchteten Cybererpressern des russischen RaaS (Ransomware-as-a-Service) Anbieter ALPHV, bzw. ihres als Scattered Spyder bekannten «Systempartners», die MGM-Casinos und -Hotels in Las Vegas zu kompromittieren. Am 13. September posteten die E-Gangster auf X, dass sie gerade einmal ein zehnminütiges Telefonat mit dem Helpdesk eines Casinos gebraucht hätten, um die Systeme des

33,9 Milliarden US-Dollar schweren US-Entertainment-Konzerns zu kontrollieren. Während zunächst MGM betont hatte, dass der Betrieb weitgehend unbeeinträchtigt sei, veröffentlichte die Gruppe am 6. Oktober die Schadensumme von 100 Millionen US-Dollar und gab bekannt, dass auch Kundendaten gestohlen worden seien. ALPHV ist auch unter dem Namen BlackCat, ALPHV-ng oder Noberus bekannt und ist seit 2021 erhöht aktiv. Die Gruppe und ihre Kunden greifen überwiegend grosse Organisationen und Unternehmen an und setzen dabei auf Triple Extortion, also auf eine dreifache Erpessung: Nach Infiltration der Systeme werden sensible Daten gestohlen. Dann verschlüsseln die Verbrecher die Systeme des Opfers und verlangen Lösegeld für die Entschlüsselung. Um der Forderung Nachdruck zu verleihen, wird mit der Veröffentlichung der gestohlenen sensiblen Daten gedroht. Und falls das Opfer immer noch nicht zahlt, droht ihm eine DDoS-Attacke. Zudem schätzen Sicherheitsforscher ALPHV als überaus professionell ein in der Anwendung von Social Engineering-Techniken, wie z.B. bei der Erbeutung geheimer Zugangsdaten durch geschickt geführte Telefonate oder emotional berührendem E-Mail-Austausch. Da die Gruppe zudem höchst routiniert mit ausserordentlich gut funktionierenden Malware-Tools arbeitet, schliessen Sicherheitsforscher und Strafverfolgungsbehörden, dass sie aus ehemaligen Mitgliedern der 2022 von russischen Behörden zerschlagenen Gruppe Cyberkriminellen REvil sowie aktiv rekrutierten BlackMatter- und DarkSide-Mitgliedern besteht.

Jüngstes Opfer in Europa: Die Motel-One-Gruppe wurde Ende September von ALPHV angegriffen. Die europäische Hotelkette mit Sitz in München betreibt die 90 Hotels in 13 europäischen Ländern. Darunter befinden sich auch je eines in Zürich und Basel. Während Motel One in einer ersten Erklärung am 2. Oktober beteuerte, es sei gelungen, die Auswirkungen des Angriffs «relativ gering» zu halten, hatten sich die Erpresser selbst damit gebrüstet, mehr als 6 Terrabyte sensible Daten in etwa 25 Millionen Files erbeutet zu haben. Darunter befinden sich Geschäftszahlen des Unternehmens, Handynummern von Angestellten, private und geschäftliche Rechnungsadressen, Geburtstage von Kundinnen und Kunden, Übernachtungslisten und die Daten von ca. 150 Kreditkarten. In den Tagen nach dem Hack stellte sich dann heraus, dass die Cyberkriminellen für einmal für sich reklamieren konnten, auf der ehrlicheren Seite zu stehen: Die Daten sind inzwischen im Darknet veröffentlicht. Motel-One-Gründer und-Mitinhaber Dieter Müller hat inzwischen eingeräumt, dass die betroffenen Kunden informiert worden seien und gegenüber der Politik beteuert, «… die Cyberabwehr erheblich aufzurüsten». Bis das erfolgt sein wird, sollte, wer seit 2016 in einem Motel One übernachtet hat, besonders vorsichtig und sensibel werden, wenn er oder sie von Unbekannten kontaktiert wird: es könnte sich um einen Phishing-Versuch handeln.

Nachzulesen unter:

https://perception-point.io/blog/stealing-more-than-towels-the-new-infostealer-campaign-hitting-hotels-and-travel-agencies
https://www.bleepingcomputer.com/news/security/hotel-hackers-redirect-guests-to-fake-bookingcom-to-steal-cards
https://www.engadget.com/hackers-claim-it-only-took-a-10-minute-phone-call-to-shutdown-mgm-resorts-143147493.html
https://twitter.com/vxunderground/status/1701758864390050145?s=46&t=mOWjpAvBR_EgMxB3MbSPxw
https://www.varonis.com/de/blog/alphv-blackcat-ransomware
https://www.bleepingcomputer.com/news/security/mgm-resorts-ransomware-attack-led-to-100-million-loss-data-theft

https://www.inside-it.ch/wir-haben-6-terabyte-daten-ransomware-bande-droht-europas-grosser-hotelkette-motel-one-20231002
https://www.golem.de/news/motel-one-hacker-stehlen-kundendaten-von-deutscher-hotelkette-2310-178139.html
https://www.netzwelt.de/news/223190-hackerangriff-motel-one-daten-millionen-gaesten-darknet-einsehbar0910.html
https://www.tagesschau.de/wirtschaft/unternehmen/motel-one-hackerangriff-100.html

III. Das NCSC warnt vor Impersonation Attacks auf die Gamer Community und neuen Fake-Sextortions

Ein ähnliches, wenn auch nicht ganz so ausgeklügeltes Angriffsmuster zeigen Attacken in der Gamer Community, vor denen das National Cyber Security Center NSCS in der Woche 40 auf seiner Website gewarnt hat: Opfer sind Mitglieder von Discord, einer Plattform, über die sich Gamerinnen und Gamer austauschen und vernetzen. Von einem kompromittierten Discord-Account aus erhalten Freunde des legitimen Account-Besitzers die Einladung, ein neues Spiel zu testen und herunterzuladen. Lädt das nichtsahnende Opfer das Spiel via Exec-Datei auf sein Device, kommt die Malware gleich dazu. Sie kann Passwörter abfangen und an die Cybergangster senden. Ist dies geschehen, versuchen diese, die Kontrolle über das Device und alle darüber gesteuerten Dienste zu übernehmen. Erkannt wurde der Schadsoftware-Befall, weil Warnmeldungen auf Versuche hinwiesen, dass Konten verändert werden sollten, was besonders in jenen Fällen misslang, in denen die Konten per 2-Faktor-Authentifzierung geschützt waren.

Weniger mit der Aussicht auf ein neues Computerspiel, sondern mit Scham und Angst arbeiten sogenannte Fake-Sextortion-Angriffe: Dabei behaupten Cyberkriminelle in massenhaft verschickten E-Mails, dass sie über Fotos oder Videos verfügen würden, die die E-Mail-Empfangsperson während eines angeblichen Besuchs auf pornografischen Websites zeigen. Im Anschluss drohen sie mit der Veröffentlichung des Bild- oder Videomaterials, falls die geforderte Lösegeldzahlung nicht innerhalb einer bestimmten Frist bezahlt wird. Um den Wahrheitsgehalt ihrer gefakten Behauptungen zu unterstreichen, verwendeten Sextortions-Angreifer oft die E-Mail-Adressen der Angeschriebenen oder von diesen verwendete Passwörter, die sie zum Versand im Darknet erwerben. Sind diese Passwörter noch aktiv, hacken die Cyberkriminellen im Anschluss gerne auch einmal die Social Media-Konten der Angeschriebenen und laden dort explizit den Inhalt hoch, um eine Sperrung der Konten zu erreichen und sie auf diese Weise zu verunsichern.

Konnte man bisher davon ausgehen, dass die in den Mails dargestellte Drohkulisse ohne Substanz aufgebaut worden ist, so berichtet das NCSC in KW 39 von einem Fall, in welchem dem Sextortion-Mail ein Screenshot des PC-Schreibtischs des Opfers sowie Daten zum Betriebssystem, mit dem der PC arbeitet, angehängt war. Woher Screenshot und Daten stammten, konnte laut NCSC bislang nicht ermittelt werden, doch schreibt die Behörde dazu: «In der neuesten Form kann nicht mehr ausgeschlossen werden, dass sich wirklich eine Schadsoftware auf den Computer eingeschlichen hat. Denn die Angreifer präsentieren als Beweis einen aktuellen Screenshot vom Computer des Opfers.»

Über eine noch raffiniertere neue Variante von Fake-Sextortion, berichtete bleepingcomputer.com Anfang September: ähnlich wie die Hospitality-Angreifer im zweiten Beitrag dieses Security Reports nutzen die Kriminellen dabei die Fake-Variante einer bekannten Webseite, um bei ihren Opfern abzukassieren. Unter «info@youporn.com» verschicken sie eine täuschend echt aussehende Nachricht an nichtsahnende Opfer, dass ein Video eben hochgeladen worden sei, welches das Opfer bei sexuellen Handlungen zeige. Weil man Sicherheit und Privatsphäre der Userinnen und User sehr ernst nehme, würden solche Videos zunächst ausgefiltert, um zu prüfen, ob das Opfer der Veröffentlichung zustimme. In diesem Fall müsse nichts unternommen werden. Wollte die oder der Angeschriebene allerdings, dass das Video nicht hochgeladen werde, solle es einem Link folgen, der zu einer gefakten YouPorn-Seite führt. Dort hat das Opfer dann die Möglichkeit, zwischen drei vermeintlichen Service-Plänen mit unterschiedlichen – dreist! – Sicherheitslevels zu wählen, die zu Preisen von 199, 699 bzw. 1'399 US-Dollar angeboten werden und auf zwei Bitcoin-Konten einzahlbar sind. Bislang, so bleepingcomputer.com, sei die Aktion erfolglos verlaufen, doch kann nicht ausgeschlossen werden, dass künftig weitere Angriffe auf ähnliche Weise erfolgen würden.

Nachzulesen unter:

https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_40.html
https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_39.html
https://www.bleepingcomputer.com/news/security/fake-youporn-extortion-scam-threatens-to-leak-your-sex-tape/

IV. Ransomware – ein Wachstumsmarkt!

Während die Wachstumsmotoren der legalen Wirtschaften in den letzten Monaten spürbar ins Stottern geraten sind, scheint der Markt für Ransomware keine Grenzen zu kennen. Das lässt sich jedenfalls aus dem Ransomware-Wochenreport auf bleepingcomputer.com vom 13. Oktober 2023 schliessen. So berichtete Autor Lawrence Abrams, dass sich die gefürchtete Cybercrime-Gruppe BianLian zum Angriff auf die Fluglinie Air Canada bekannt hat. Die hier schon mehrfach erwähnte APLHV-Gruppe hat eine Reihe von Gerichten in Nordwest-Florida angegriffen. Und mit Simpson Manufacturing sah sich einer der grössten Hersteller von strukturellen Verbindungselementen in den USA gezwungen, nach einem Cyberangriff alle IT-Systeme herunterzufahren und neu aufzusetzen. Abrams betont, dass in diesem Fall nicht klar ist, ob es sich bei dem Angriff um einen Erpressungsversuch oder einen reinen Sabotageakt gehandelt hat.

Mit 1’420 Fällen haben die Cybererpresser im dritten Quartal 2023 ihre Rekordzahl von 1’386 Fällen aus dem zweiten Vierteljahr 2023 nochmals übertroffen. Neben diesen Zahlen zeigt der «Ransomware Trends Q3 2023»-Report des Security-Unternehmens cyberint (unten verlinkt) in einer gut zusammengestellten Übersicht, dass neben den «Branchengrössen» wie Lockbit3, ALPHV und BianLian erfolgreiche Newcomer wie Clop vor allem in den westlichen Industrienationen aktiv waren. Mit 616 erfolgreichen Angriffen sind die USA in beinahe der

Hälfte aller Fälle das Angriffsziel. Mit weitem Abstand folgten das Vereinigte Königreich, Kanada, Deutschland und Frankreich. Interessanterweise konzentrierten sich die Angriffe primär auf Zulieferer und Business Service Provider, gefolgt von industriellen Herstellern und dem Einzelhandel. Und auch, wenn die Schweiz nicht unter den Top 10 der angegriffenen Länder zu finden ist – was für einmal ja auch gar nicht erstrebenswert ist – so sind doch auch hierzulande Lockbit3, ALPHV, Clop und BianLian als Angreifergruppen aktiv.

Angesichts des Ausblicks im cyberint-Report verheisst das für die legale Welt nichts Gutes: Neue Gruppen wie die Rhysida Ransomware Group, 3AM oder eben Clop machen den «Veteranen» wie Lockbit3 oder ALPHV keine Konkurrenz, sondern erweitern einfach das Angriffsfeld. Investitionen in Cybersicherheit und Awareness sind daher sicher auch für Schweizer Institutionen und Unternehmen eine kosteneffiziente Art, Geld und Ressourcen einzusetzen.

Nachzulesen unter:

https://www.bleepingcomputer.com/news/security/simpson-manufacturing-shuts-down-it-systems-after-cyberattack
https://cyberint.com/blog/research/ransomware-trends-q3-2023-report

V. In eigener Sache: Weiterentwicklung des SWITCH Security Reports

Es freut uns sehr, dass Sie zum Empfangskreis des Security Reports gehören. Mit Ihrer Meinung entscheiden Sie mit, in welche Richtung wir dieses Informationsprodukt weiterentwickeln. Bitte nehmen Sie sich dazu 1 Minute Zeit und beantworten Sie vier Fragen.

Mit diesem Link gelangen Sie direkt zur Umfrage.

Vielen Dank für Ihre Teilnahme.

Dieser SWITCH Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.