2020 Bedrohungsbericht für Finanzdienstleister und Versicherungen

EINFÜHRUNG

Die weltweite Pandemie hat zahlreiche Finanzdienstleister und Versicherungen dazu veranlasst, ihre Digitalisierungsmaßnahmen zu beschleunigen. Diese Maßnahmen haben viel Positives bewirkt. Dazu gehören optimierte, routinemäßige Remote Customer Journeys, eine skalierte Infrastruktur zur einfacheren Erweiterung des Perimeters sowie Einrichtungen für sich rasch ändernde Kommunikations- und Compliance-Anforderungen. Diese Änderungen haben dazu beigetragen, dass Bank- und Vermögensberater sowie Händler und Vermittler Märkte und Finanzbewegungen einfacher verwalten können. Gleichzeitig bieten sie aber auch Bedrohungsakteuren neue Gelegenheiten.

Bedrohungsakteure nutzen jede Gesellschaftskrise blitzschnell aus – COVID-19 bildet dabei keine Ausnahme. Der Sektor der Finanzdienstleister und Versicherungen hat den herkömmlichen Netzwerk-Perimeter hinter sich gelassen – und die Angreifer sind ihr gefolgt. Die Bedrohungen sind jedoch nicht nur beweglich, sondern nehmen auch andere Formen an und wählen neue Ziele aus. Jeder Mitarbeiter in Ihrem Unternehmen stellt ein anderes Sicherheits- bzw. Compliance-Risiko dar. Dies ist durch die Daten bedingt, auf die die betreffende Person Zugriff hat, und durch die Art und Weise, wie sie die vorhandenen Technologie nutzt.

Um Führungskräften von Finanzdienstleistern und Versicherungen einen besseren Überblick über die sich verändernde Bedrohungslandschaft zu ermöglichen, haben wir die Daten des vergangenen Jahres analysiert und uns dabei auf das erste Halbjahr 2020 konzentriert. Proofpoint Threat Research untersuchte tausende Bedrohungskampagnen mit Millionen Nachrichten. In diesem Bericht werden die Ergebnisse dieser Untersuchungen vorgestellt und mit Daten, realen Beispielen und Erkenntnissen ergänzt, um zu zeigen, welche Bedrohungen auf den Sektor Finanzdienstleistungen und Versicherungen abzielen.

Zielgruppe und Ziel

Dieser Bericht richtet sich an Führungskräfte sowie leitende Sicherheitsverantwortliche bei Finanzdienstleistern und Versicherungen und ist darauf ausgerichtet, das Risiko zu reduzieren, dem diese Unternehmen ausgesetzt sind, wenn es um personenbezogene Informationen, Finanzdaten, geistiges Eigentum, nicht öffentliche Informationen, externe FSI-Ökosysteme (Financial Services and Insurance) und Betrug geht. Zudem soll der Bericht helfen, Angestellte bei Finanzdienstleistern und Versicherern zu Themen wie Sicherheitsbewusstsein sowie Sicherheit zu schulen.

Methoden der Untersuchung

Für diese Untersuchung wurden Proofpoint-Daten zu Bedrohungsakteuren, Kampagnen, BEC-Angriffen (Business Email Compromise, auch als Chefmasche bezeichnet) und Very Attacked People™ (VAPs) aus dem 4. Quartal 2019 und dem ersten Halbjahr 2020 analysiert. In einigen Fällen nutzen wir öffentlich verfügbare Informationen, um Sicherheitsthemen zu untersuchen, die wir in den Proofpoint-eigenen Daten nicht direkt beobachten konnten.

Inhaltsverzeichnis

Kurzfassung

Der Sektor der Finanzdienstleister und Versicherer ist ein permanentes Ziel für böswillige Akteure, ganz gleich, ob ihr Motiv Betrug, Hacktivismus oder Terrorismus ist. Der Bericht kommt zu den folgenden wesentlichen Erkenntnissen:

Der häufigste Angriffsvektor ist der Mensch, nicht Technologie.

Laut Proofpoint Threat Intelligence beginnen mehr als 96 % aller Angriffe mit Social Engineering, dem Vortäuschen falscher Tatsachen, Phishing und Bedrohungen durch Insider, während zahlreiche Unternehmen den Großteil ihres Budgets für technologiebasierte Lösungen aufwenden.

Basierend auf der von Proofpoint durchgeführten Analyse der Kompromittierungsindikatoren (Indicators of Compromise, IoCs) sowie der Taktiken, Techniken und Prozeduren (TTPs) lässt sich eine Liste der besonders häufig angegriffenen Personen (Very Attacked People, VAPs) unter dem allgemeinen Mitarbeiterstamm ableiten. Dadurch können Sicherheitsmaßnahmen entsprechend angepasst werden.

Bedrohungsakteure reagieren schnell auf neue Umgebungsbedingungen.

Aus dem Verizon Data Breach Incident Report für das Jahr 2020 geht hervor, dass sich Cloud-basierte Angriffe im vergangenen Jahr verdoppelt haben. Gleichzeitig ist die Anzahl der Mitarbeiter im Home Office gestiegen.

Bedrohungsakteure im Finanzsektor verfolgen eine extrem fokussierte Strategie, gehen äußerst methodisch vor und kennen ihre Ziele genau.

Lieferkettenrisiken nach der zweiten Ebene sind kaum kontrollierbar.

Die Lieferkette im Finanzsektor unterliegt weltweit – mehr als in allen anderen Sektoren – starken wirtschaftlichen Schwankungen. Sie umfasst Börsen, Clearinghäuser und Zentralbanken mit internationaler Tragweite.

Die Sicherheitsanforderungen für Lieferketten sind unterschiedlich. Wenn Sie die Einhaltung von Sicherheitsmaßnahmen durch Ihre Lieferanten der ersten und zweiten Ebene erzwingen möchten, indem Sie Ihre internen Anforderungen schlicht auf sie übertragen, können Sicherheitslücken für den Lieferanten entstehen. Dem Lieferanten wird es unter Umständen unmöglich, Ihr Unternehmen ordnungsgemäß zu bedienen.

Jedes Marktsegment hat eine spezifische Bedrohungslandschaft.

Aus den Daten von Proofpoint Threat Intelligence sowie aus unabhängigen Berichten geht hervor, dass die IoCs und TTPs je nach Marktsegment variieren. Die Abwehr von Bedrohungen muss also an jedes einzelne Marktsegment angepasst werden.

Kryptowährungen sind im Anmarsch.

Das Office of the Comptroller of the Currency (OCC) hat vor Kurzem eine Erklärung veröffentlicht, wonach Bankinstitute berechtigt sind, digitale Schlüssel für Kryptowährungsgeldbörsen aufzubewahren.

Wenn Banken berechtigt sind, digitale Vermögenswerte für ihre Mandanten aufzubewahren, gehen die gesetzlichen Pflichten und Cybersicherheitsrisiken im Zusammenhang mit diesen Kryptowährungen auf diese Banken über.

Finanzdienstleistungen und Versicherungen – Sicherheit und Bedrohungsmetriken

Die Finanzdienstleistungsbranche verfügt über mehrere einzigartige Merkmale, die Bedrohungsakteure anziehen wie ein Magnet:

HOHE BELOHNUNG

Die Rentabilität eines Angriffs gegen ein Finanzdienstleistungsunternehmen ist höher als in anderen Sektoren, da hier naturgemäß viel Kapital vorhanden ist.

STARKE AUSWIRKUNG

Jeder Angriff kann unabhängig von seinem Ausmaß eine Schlagzeile wert sein und eine Marktreaktion hervorrufen. Die Wirkung kann sich rasch von einem einzelnen Unternehmen auf die gesamte Weltwirtschaft ausweiten.

REGULIERT

Dadurch, dass klar definierte Regulierungsprozesse und Verfahren einzuhalten sind, reduziert sich der Aufklärungsbedarf des Kontrahenten hinsichtlich seines Ziels.

LEGACY-TECHNOLOGIE

Oft kommt veraltete IT zum Einsatz. Das Sicherheitsrisiko ergibt sich etwa aus der Einstellung des Supports durch den Hersteller oder aus proprietären Systemen, die sich infolge von Fusionen und Übernahmen angesammelt haben. Ein ebensolches Risiko stellen Systeme dar, deren Aktualisierung als zu komplex erachtet wird oder ausgesetzt wurde, weil einfach das entsprechende Know-how für diese Legacy-Systeme fehlt.

INFRASTRUKTURDSCHUNGEL

Da Fusionen und Übernahmen von je her typisch für den Sektor sind, ist eine gewisse Komplexität und Unübersichtlichkeit entstanden. Lockere Integrationen zwischen an sich getrennten Systemen haben zu einer verzweigten Infrastruktur geführt, die eine breitere Angriffsfläche bietet und mehr Ressourcen für Sicherheitsüberwachung und Abwehr erfordert.

CLOUD-/CONTAINER-TECHNOLOGIE

Das Hochladen von Legacy-Anwendungen in die Cloud (oder in Container) kann dazu führen, dass bislang unbekannte Schwachstellen ausgenutzt werden. Aufgrund der Bereitstellungsmechanismen können auch neue Schwachstellen entstehen. Die Beauftragung neuer SaaS-Anbieter zum Auslagern nicht kritischer Systeme kann neue Angriffsflächen mit lediglich begrenzten Möglichkeiten zur Handhabung von Zwischenfällen eröffnen.

HOHER AUTOMATISIERUNGSGRAD

Unternehmen im Bereich Finanzdienstleistungen und Versicherung setzen verstärkt auf Automatisierung, um Kosten zu senken und Legacy-Systeme zu modernisieren. Die Verbreitung von standardisierter Automatisierung erhöht jedoch die Anfälligkeit, wenn Unternehmen von einem solchen Legacy-System abhängig sind, die Geschäftslogik komplexer wird oder es an Dokumentation fehlt.

Zu dieser Branche gibt es einige wichtige Statistiken zu Sicherheitsprävention, neuen Bedrohungen und persistenten Angriffen:

Security Awareness-Training

Finanzdienstleister und Versicherer sind sich im Vergleich zu anderen Branchen etwas bewusster über Bedrohungen durch Insider sowie über Bedrohungen in Verbindung mit Kontoauthentifizierung.

- Finanzdienstleister weisen eine Fehlerquote von 20 % auf, während es im Durchschnitt 22 % sind.
- Besser schneiden Finanzdienstleister bei der „Identifizierung und Verhinderung von Insider-Bedrohungen“ und im Bereich „Kontoauthentifizierung“ ab.
- Schlechter steht es lediglich in den Kategorien „Schutz vor physischen Risiken“ und „Vermeidung von Ransomware-Angriffen“.

E-Mail-Bedrohungen

Die Anzahl der URL-Bedrohungen war durchgängig höher als die der Angriffe mit schädlichen Anhängen.

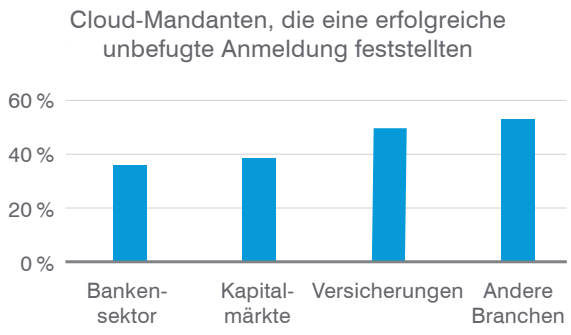
- 82 % aller schädlichen Nachrichten in der Finanzdienstleistungsbranche enthielten URLs.
- 72 % der Angriffe basierten auf Malware.

Cloud-Zugriff

Social-Engineering-Taktiken zum Erlangen von Cloud-Zugriff weisen eine beeindruckende *Erfolgsquote von 75* % auf, während es bei Brute-Force-Angriffen nur etwa 9,7 % sind. Auf den Menschen ausgerichtete Angriffe versprechen den Bedrohungsakteuren also ganz klar die höchste Rendite.

Im Versicherungsbereich funktioniert die unbefugte Anmeldung besser als bei Banken oder Kapitalmärkten.

- 72 % der Unternehmen waren Ziel von Brute-Force-Methoden, allerdings führten nur 7 % dieser Attacken zum Erfolg.
- 28 % waren Ziel von Social-Engineering-Taktiken. 21 % wurden erfolgreich unter Anwendung per Phishing kompromittiert.



Data Loss Prevention (DLP) und Bedrohungen durch Insider

Jeder Teilbereich des Finanzdienstleistungs- und Versicherungssektors weist eine eigene Quote für Bedrohungen durch Insider auf. Aus einer Untersuchung zu Insider-Zwischenfällen von 1996 bis 2018 geht hervor, dass der Bankensektor bei weitem am fahrlässigsten war.[1]

Segment	Gruppe(n)	Risiken durch Insider-Bedrohungen	Anzahl der Insider-Zwischenfälle[2]
Bankensektor	Sparkassen, Kreditwesen, Finanzen	Personenbezogene Daten, Kontoübernahme	190
Kapitalmärkte	Investment Banking, Asset Management	Geistiges Eigentum, Fusionen und Übernahmen, Insidergeschäfte	Keine Daten verfügbar
Versicherungen	Haftpflicht, Eigentum und Schaden	Personenbezogene Daten, Versicherungsbetrug	14
Ökosystem	Börsen, Zahlungsabwickler, Marktdaten, Cloud/SaaS, Lieferkette	AML, Gegenpartei, SWIFT, ACH, Marktmanipulation	33

TTPs bei Insider-Zwischenfällen im Finanzdienstleistungssektor

CERT hat in Zusammenarbeit mit DHS und USSS Insider-Zwischenfälle von 2005 bis 2012 untersucht und ist dabei folgender Frage nachgegangen: „Welches sind die technischen und verhaltensbasierten Vorläufer von Insider-Betrug im Finanzsektor und welche Abhilfestrategien bieten sich an?“[3] Die Untersuchung führte zu den folgenden wesentlichen Ergebnissen:

Der Ansatz „low and slow“ verursachte höheren Schaden und wird später erkannt.

Anomaliegestützte Technologielösungen haben sich nicht nur als ineffektiv, sondern sogar als kontraproduktiv erwiesen, da die langfristigen schädlichen Aktivitäten als Teil der Benutzerbasislinie eingestuft wurden.

Die Mittel der Insider waren technisch nicht hoch entwickelt.

Das Fehlen von ausgeklügelter Technologie bewirkt, dass vorhandene Sensordaten einem Insider-Bedrohungsprogramm zugeführt werden können. Der Trick liegt in der Analyse des Benutzerverhaltens.

Betrug durch Führungskräfte unterscheidet sich in Bezug auf Schaden und Dauer erheblich vom Betrug durch andere Mitarbeiter.

Führungskräfte haben die Möglichkeit, Geschäftsprozesse zu verändern, um sich finanzielle Vorteile zu verschaffen. Dies erfolgt unter anderem durch Manipulieren unterstellter Mitarbeiter. Bei den Nicht-Führungskräften handelt es sich oft um Kundendienstmitarbeiter, die Konten modifizieren oder personenbezogene Daten von Kunden zu ihrem Vorteil nutzen.

Die meisten Zwischenfälle kamen aufgrund einer Prüfung, einer Kundenbeschwerde oder eines Verdachts seitens eines Kollegen ans Tageslicht.

Dies ist eine wichtige Erkenntnis: Während ein externer Angriff eine Spur von anormalen „Brotkrumen“ hinterlässt, basiert die Insider-Bedrohung auf Stimmungen, Beweggründen und Geisteshaltungen – Faktoren, die nur schwer mittels Technologie erkannt werden.

Wolf im Schafspelz

In einigen Fällen gibt es auch eine direkte Verbindung zwischen der Insider-Bedrohung und dem Unternehmen, das mit der Untersuchung von Insider-Bedrohungen beauftragt ist. 2019 wurde ein ehemaliger Securities Compliance Examiner der US-Börsenaufsichtsbehörde SEC beauftragt, im Rahmen einer laufenden Untersuchung auf Informationen einer Beteiligungsfirma zuzugreifen. Er machte sich sein Wissen zu Nutze, um die Position des Chief Compliance Officer in dem Unternehmen zu ergattern.[4] Die Tatsache, dass der Betreffende aus der Compliance kam und genau in diesem Bereich wieder tätig wurde, ist nicht nur eine Ironie, sondern zeigt auch, dass bei Insider-Bedrohungen keine moralischen Hemmungen bestehen.

[1] Miller & Trotman (2018): „Insider Threats in Finance and Insurance (Part 4 of 9: Insider Threats Across Industry Sectors)“ (Insider-Bedrohungen im Finanz- und Versicherungssektor: Teil 4 von 9 – Insider-Bedrohungen in verschiedenen Branchen), CMU SEI.

[2] ebd.

[3] Cummings, Lewellen, McIntire, Moore & Trzeciak (2012): „Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector“ (Umfrage zu Insider-Bedrohungen: Unrechtmäßige Cyberaktivitäten mit Betrug im US-Finanzdienstleistungssektor), CMU SEI, DHS S&T, USSS and CERT Insider Threat Center.

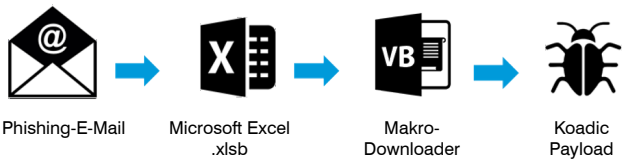
[4] Godoy & Lorenzo (2019): „Ex-SEC Compliance Expert Denies Pilfering Info For PE Firm“ (Ehemaliger SEC-Compliance-Experte streitet Weitergabe von Informationen an Private-Equity-Firma ab), Law360.

Häufige Taktiken bei Angriffen auf Finanzdienstleister und Versicherer

Proofpoint Threat Intelligence hat festgestellt, dass bestimmte Taktiken von Bedrohungsakteuren zugenommen haben:

VBA Stomping

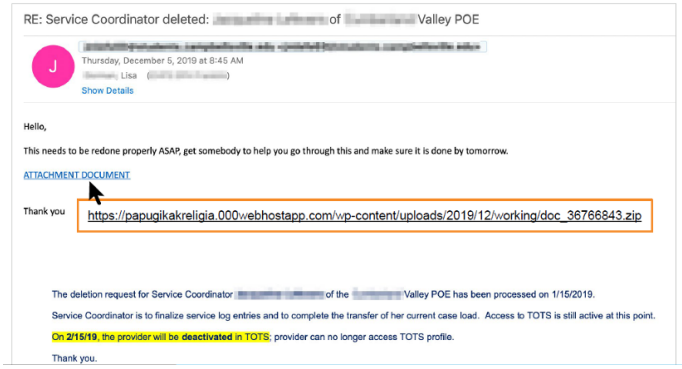
Diese Taktik mit schädlichen Anhängen präsentiert Sicherheitsanalysemodulen einen anderen (ausführbaren) VBA-Code als der, der tatsächlich ausgeführt wird. Dabei werden zahlreiche Tools für Code-Signaturerkennung und heuristische Erkennung umgangen.



Thread-Hijacking

Diesem BEC-Verfahren (Business Email Compromise), bei dem falscher E-Mail-Inhalt (schädliche URLs) in einen vorhandenen E-Mail-Thread injiziert wird, fallen viele Benutzer zum Opfer. Der E-Mail-Thread ist bereits vorhanden und suggeriert Vertrauen. Viele Opfer sind daher geneigt, die E-Mail zu öffnen und auf die enthaltenen Links zu klicken.

Eine weitere Taktik, die auf diesem Verfahren basiert, ist das Einbetten schädlicher URLs in den Abschnitt „ursprüngliche Nachricht“ der E-Mail. Viele Tools für E-Mail-Sicherheit führen dort keine Prüfung mehr durch. Auch hier werden viele heuristische Erkennungstools umgangen.


RE: Service Coordinator deleted: [redacted] of [redacted] Valley POE

[redacted]

Thursday, December 5, 2019 at 8:45 AM

[redacted] Lisa [redacted])

Show Details

Hello,

This needs to be redone properly ASAP, get somebody to help you go through this and make sure it is done by tomorrow.

ATTACHMENT DOCUMENT

Thank you https://papugikakreligia.000webhostapp.com/wp-content/uploads/2019/12/working/doc_36766843.zip

The deletion request for Service Coordinator [redacted] of the [redacted] Valley POE has been processed on 1/15/2019.

Service Coordinator is to finalize service log entries and to complete the transfer of her current case load. Access to TOTS is still active at this point.

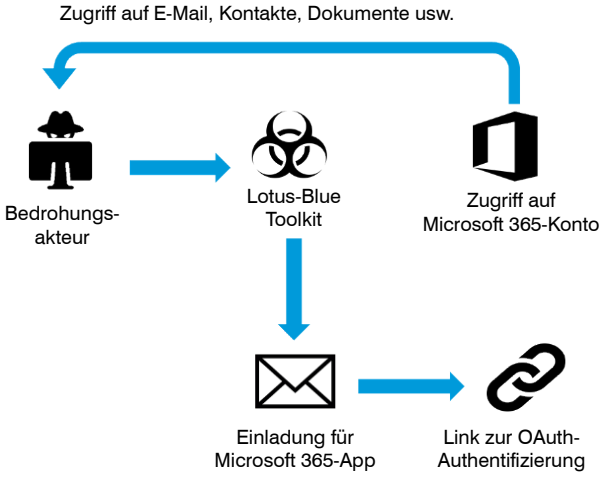
On 2/15/19, the provider will be deactivated in TOTS; provider can no longer access TOTS profile.

Thank you.

Bei Emotet, der produktivsten Malware der letzten beiden Jahre, automatisierten die Akteure den Vorlagenprozess. Dadurch wurde diese Technik in einer unglaublichen Größenordnung eingesetzt, während normalerweise ein gewisses Maß an direkter Analyse und Anpassung durch die Bedrohungsakteure erforderlich ist.

Manipulierte Drittauthentifizierung (3rd Party Authentication, 3PA)

Diese Kontoübernahme-Taktik (Account TakeOver, ATO) verwendet typisches DNS Twisting, um Benutzer dazu zu verleiten, SAML-basierte Token-Berechtigungen für die Cloud-Anwendungen eines Benutzers preiszugeben (z. B. Microsoft 365, Google Workspace). In der Regel beginnt dies als BEC und entwickelt sich rasch zu einem EAC (Email Account Compromise).
Der Zugriff auf das E-Mail-Konto eines Benutzers ermöglicht die Kennwortzurücksetzung für andere Anwendungen und es entsteht eine komplette ATO.



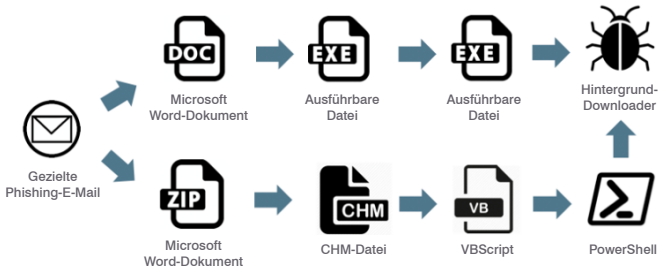
Besonders schädlich wird diese Art von ATO dadurch, dass das Ändern des Kennworts oder die Verwendung von MFA keinen Unterschied macht, sobald ein Konto angegriffen wurde. Die einzige Möglichkeit, den Zugriff des Bedrohungsakteurs zu unterbinden, besteht in der expliziten Entfernung der Token-Berechtigungen. Diesen Prozess kennen die meisten Endnutzer jedoch nicht.

Mehrschichtiger Dateifreigabeangriff

Bei dieser Taktik wird ein gehostetes Dokument präsentiert, das wiederum auf Schichten von Dokument-URLs verweist, die auf vielen unterschiedlichen Dateifreigaben gehostet werden. Dies führt letztendlich zu Malware-Schaddaten.

Da immer mehr Finanzdienstleister Cloud-basierte Dateifreigaben (und 3PA) nutzen, kommt dieses Verfahren immer häufiger zur Anwendung.

Beispiel: Schaddaten (ein VB-Skript, das den eingebetteten Bank-Trojaner Ursnif lädt) werden per Kennwort geschützt (verschlüsselt), wobei das Kennwort im Textteil der E-Mail verwendet wird.



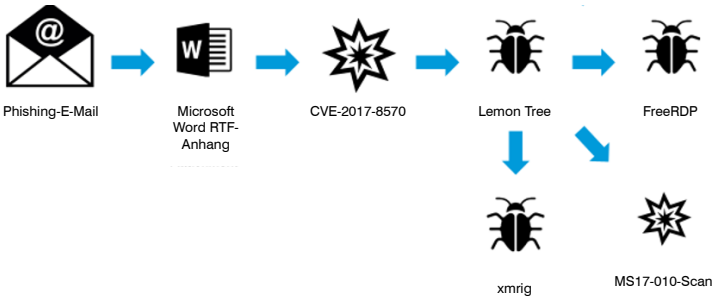
Einerseits erscheint das Hinzufügen von Schritten wie der erzwungenen Kennworteingabe durch das Opfer nicht intuitiv. Je mehr Schritte erforderlich sind, desto höher die Wahrscheinlichkeit, dass ein Schritt falsch durchgeführt wird oder der Benutzer vorzeitig aufgibt.

Andererseits wird dadurch das direkte Scannen des Anhangs verhindert. Bei den Schutzlösungen mussten daher Verfahren implementiert werden, die entweder mit einem immer größeren Wörterbuch mit häufig verwendeten Kennwörtern einhergingen (Akteure möchten diese aus oben genanntem Grund einfach halten und ändern sie nicht für jede Kampagne) oder mit dem Scannen und Analysieren von Textteilen (was in großem Umfang schwierig ist).

Manchmal besteht das Kennwort aus einem Bild statt aus Text. Letztere Methode, bei der nach Textkennwörtern gescannt wird, würde demnach nicht funktionieren.

„Living-off-the-Land"-Angriffe (dateilos/serverlos)

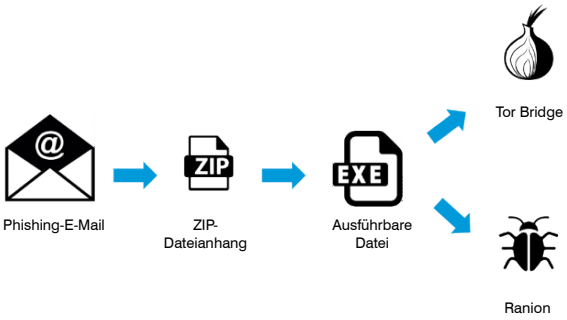
Bei diesem Angriffs werden vorhandene Funktionen innerhalb des Zielbetriebssystems (z. B. PowerShell) genutzt, um Schaddaten auszuführen. Die Schaddaten selbst sind nicht binär, sodass sie sowohl signaturbasierte als auch heuristische Erkennungsmethoden entgehen.



Ransomware-as-a-Service (RaaS)

Ransomware-Plattformen wurden ähnlich wie viele andere Angriffsplattformen standardisiert.

Ransomware-Plattformanbieter sind zu einem Abonnementdienst übergegangen und verlangen nicht mehr einen Anteil der Zahlung. Dadurch wird RaaS nicht nur attraktiver als andere Angriffsplattformen, sondern auch die RaaS-Anbieter werden von einer direkten Mitschuld an kriminellen Handlungen befreit. (Dies wäre anderenfalls so, als würde man Waffenhersteller für jede abgefeuerte Kugel rechtlich belangen.)



Neuere Iterationen dieses Dienstes beinhalten die automatische Installation von TOR-Clients auf den Computern der Opfer, um den Opfern zu Zahlung des Lösegelds zu vereinfachen.

Finanzdienstleistungsbranche – Erkenntnisse

Bankensektor

Der Bankensektor hat in den letzten Jahren am meisten von Innovation und Fortschritt profitiert – von mobilen Transaktionen über API-fähige Dienste bis hin zur Verarbeitung auf Basis von künstlicher Intelligenz (KI). Mit den neuen Technologien halten auch neue Angriffsmethoden Einzug, doch die Motive und Ziele der Bedrohungsakteure bleiben die gleichen. Accenture geht davon aus, dass im Bankensektor rund 347 Milliarden US-Dollar auf dem Spiel stehen.[5]

ÜBERSICHT: BESONDERHEITEN IM BANKENSEKTOR	
VAPs:	**Breit angelegtes Phishing**: • Technologieteam • Führungsebene **Gezielte Business Email Compromise (BEC)-Angriffe:** • Relationship Manager • Investor Relations/Finanzberater • Business Development
Ziele:	• Kunden (direkt) • Mitarbeiter (direkt) • Kunden (indirekt): Mitarbeiter mit Zugriff auf Kundendaten/-systeme • Mitarbeiter (indirekt): Mitarbeiter mit Zugriff auf Personaldaten/-Systeme
Absichten:	• Finanzielle Verluste des Kunden

Bankensektor: Gezielte Angriffe

Proofpoint Threat Intelligence hat Angriffe identifiziert, die sich gegen eine spezifische Rolle oder Firma richten. Das deutet auf ein klar definiertes Ziel hin, das durch firmenspezifische Erkundungen ausfindig gemacht wurde.

Großes Bankinstitut

Analystenkommentar: Ein Fortune 100-Bankinstitut erhielt 12 Nachrichten (100 %), bei denen unter Verwendung eines neuen WhiteShadow[6]-Verfahrens ein unbekannter Satz Malware bereitgestellt wurde. Dies ist in mehrfacher Hinsicht interessant.

Die Tatsache, dass die Malware nicht identifiziert wurde, könnte ein Hinweis darauf sein, dass die Firma nur ein Test für einen größeren, systematischen Angriff war.

WhiteShadow wird häufig für die Verteilung von Crimson verwendet, einen Remote-Zugriffs-Trojaner (RAT), der 2016 erstmals identifiziert wurde. Die Schaddaten werden von einer pakistanischen APT-Gruppierung mit dem Namen „Transparent Tribe“ verbreitet.[7] Seit dieser Zeit wurde Crimson RAT von einer Reihe krimineller Akteure standardisiert, allerdings wird Proofpoint Threat Intelligence des öfteren von Bankinstituten gefragt, ob es sich bei der Angriffskette von WhiteShadow zu Crimson nicht um eine staatlich unterstützte Maßnahme handeln könnte.

Instanzen der WhiteShadow-Technik, bei denen andere Malware als Crimson über eine Infrastruktur installiert wird, die nicht explizit mit dem pakistanischen Netzwerk verbunden ist, legen nahe, dass die Entwicklung des Verfahrens und der zugehörigen Schaddaten noch nicht abgeschlossen ist.

Kreditgenossenschaft: Lieferkettenangriff

Analystenkommentar: Eine Kreditgenossenschaft erhielt 67 Nachrichten (87 %), ebenso wie mehrere regionale Wirtschaftsprüfungsgesellschaften. Ein Zusammenhang zwischen der Kreditgenossenschaft und diesen Gesellschaften könnte ein Hinweis auf einen Seitenkanal-/Lieferkettenangriff sein.

Die beabsichtigte Schaddatenkette von GuLoader QuasarRAT wirft keine großen Fragen auf, ist jedoch ein Beispiel für einen groß angelegten TTP-Wechsel innerhalb der gesamten Bedrohungslandschaft in den letzten zwei Jahren. Bislang bestand das Ziel lediglich darin, den Grundstein für die Bereitstellung weiterer Schaddaten zu legen. Als Open-Source-Tool bietet QuasarRAT raffinierten Akteuren zudem die Möglichkeit, die Attribution zu verschleiern. Gelingt es beispielsweise einem Bedrohungsakteur, sich Zugang zu einem System mit generischer/weit verbreiteter Software zu verschaffen, lässt sich wesentlich schwieriger feststellen, von wem der Angriff tatsächlich ausgeht. Nach einem erfolgreichen Angriff kann der Akteur mithilfe dieses Verfahrens nach einiger Aufklärung weitere Schaddaten bereitstellen.

[5] Accenture (2020); „The State of Cybercrime in Banking and Capital Markets“ (Der Stand bei Cyberkriminalität bei Banken und Kapitalmärkten).

[6] https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

[7] https://www.proofpoint.com/us/threat-insight/post/Operation-Transparent-Tribe

Bankensektor: Bedrohungsanalyse und Trends

Über einen Zeitraum von sechs Monaten (vom 4. Quartal 2019 bis zum 2. Quartal 2020) hat Proofpoint Threat Intelligence die in Abbildung 1 dargestellten Bedrohungen überwacht, die sich konsequent gegen Banken richten.

Überweisungen

Analystenkommentar: In diesem Fall erhält der Bereich Handelsbanken fast doppelt so viele Nachrichten wie die nächste Branche in der Rangliste. Dennoch erhalten auch Kunden aus den Bereichen Finanzbeteiligung, Finanztransaktionen und dem Finanzökosystem Nachrichten. Die Nachrichten werden relativ gleichmäßig auf viele Institute und Regionen und nicht nur auf einige wenige Kunden verteilt. Die Masche basiert auf dem Vortäuschen einer Geldüberweisung von Western Union mit dem Ziel, einen RAT einzuschleusen. Im Betreff geht es angeblich um Compliance.

Sonstige Kampagnen

TeamViewer Bot (MINEBRIDGE) | Word-Dokumente | „Indeed-Bewerbung: Vollzeit-Kassierer“
Breit angelegter Angriff gegen Finanzdienstleister mit scheinbaren Bewerbungen als „Vollzeit-Kassierer“ mit gefälschtem Absender einer Personalvermittlung.

GuLoader / Parallax „warii“ | Anhänge | „MAJ Code Banques“
Die Nachrichten enthalten Microsoft Office-Anhänge mit Makros, die bei Aktivierung GuLoader herunterladen und ausführen. Dadurch wiederum wird Parallax heruntergeladen und installiert. Banken und Dienstleistungsunternehmen waren das primäre Ziel.

jSocket „88.150.189[.]98“ | URLs | „Steuerrückzahlung“
Diese Nachrichten enthalten URLs, die zu einer komprimierten Java-Datei führen. Fast alle Nachrichten wurden an ein Bankunternehmen gesendet.

Get2 / SDBbot | Excel-Dokumente
E-Mails mit Microsoft Excel-Anhängen beinhalten Makros, die bei Aktivierung eine eingebettete DLL-Datei ausführen („Get2“ Loader-Malware). Über Get2 wird SDBbot und unbekannte Malware geladen. Banken waren das primäre Ziel – 76 % der Nachrichten in dieser Kampagne wurden an die Finanzdienstleister gesendet. Diese Kampagne richtete sich im Dezember 2018 und Januar 2019 gegen Bankunternehmen. Bankunternehmen sind nach wie vor häufige Ziele.

URLs | Word-Dokumente | PDF-Dateien
Die USA sind Ziel von E-Mails, die URLs, Word-Dokumente oder PDF-Dateien enthalten. Dabei missbrauchen die PDF-Dateien die Markennamen zahlreicher Fortune 100-Banken. Die zahlungsbezogene Nachricht lockt durch die Verwendung des Namens eines Einzelhandelsunternehmens gezielt Finanzdienstleister in die Falle.

CobInt | Cobalt-Gruppe | URLs
Die Nachrichten enthalten Links zu einer PDF-Datei, die auf Microsoft OneDrive gehostet wird und Links enthält, über die eine Datei mit dem Namen „Documents.rtf“ heruntergeladen wird. Dieses Dokument enthält Exploits, die bei erfolgreicher Ausführung CobInt herunterladen. In den USA waren mehrere Angestellte Zielscheibe der CobInt-Malware, die zur Gruppe der Backdoor-Trojaner und Downloader gehört. Der Angriff ging von einem überwachten Bedrohungsakteur aus, der seine Opfer vorrangig im Bereich Banking/Darlehen sowie in der Medien- und Unterhaltungsbranche suchte. In diesem Fall wurden mehr als 50 % der E-Mails an Mitarbeiter im Finanzdienstleistungssektor gesendet. Diese Gruppe war damit größtes Ziel.

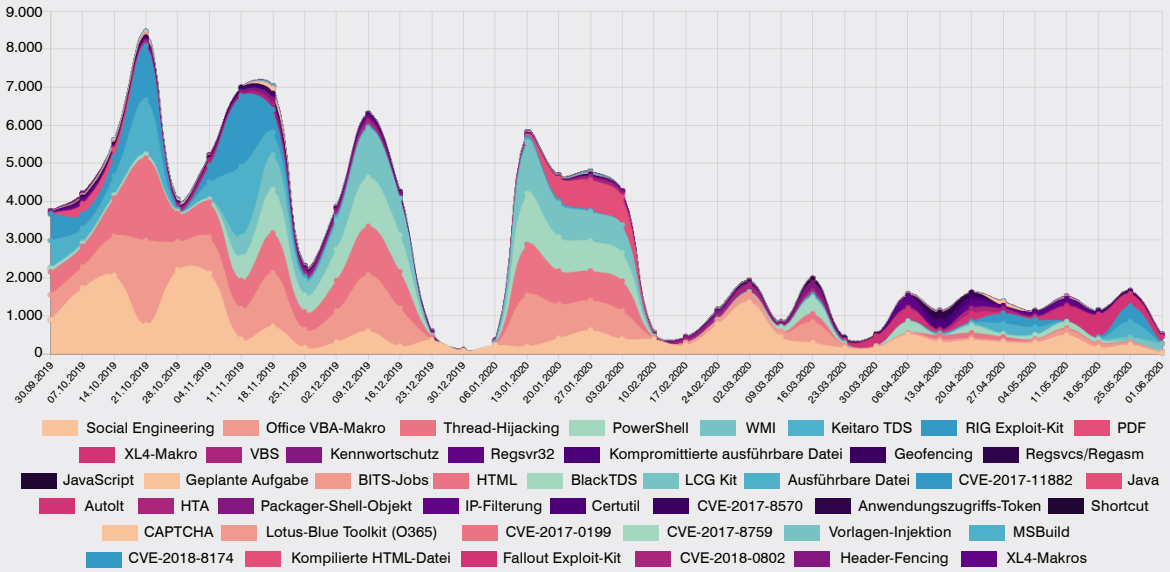


Abb. 1: Sparkasseninstitute – Gezielte Exploits (Quelle: Proofpoint).

Kapitalmärkte

Accenture schätzt, dass rund 47 Milliarden US-Dollar auf dem Kapitalmarkt aufgrund von Cyberangriffen in Gefahr sind.[8]

ÜBERSICHT: BESONDERHEITEN DES KAPITALMARKTSEKTORS	
VAPs:	**Breit angelegtes Phishing**: • Technologieteam • Führungskräfte/Managing Partner **Gezielte BEC-Angriffe:** • Finanzberater/Analysten • Fondsmanager/Portfoliomanager • Forschungsdirektor
Ziele:	• Kapital/Vermögenswerte (direkt): Mitarbeiter mit Zugriff auf Vermögenswerte • Kunden (indirekt): Mitarbeiter mit Zugriff auf Kundendaten/-systeme
Absichten:	• Disruption des Sektors • Markt-/Wirtschaftsdisruption

Kapitalmärkte: Gezielte Angriffe

Proofpoint Threat Intelligence hat Angriffe identifiziert, die sich gegen eine einzelne Rolle oder Firma richten. Das deutet auf ein klar definiertes Ziel hin, das durch firmenspezifische Erkundungen ausfindig gemacht wurde.

Obskure Schaddaten möglicherweise Vorreiter

Wenngleich bei diesen speziellen Angriffen unscheinbare Köder verwendet wurden (z. B. Versandrechnungen, Paketverfolgung und Steuer-Themen), gab es eine Neuerung: Die Schaddaten erforderten NodeJS für die Ausführung. NodeJS ist eine beliebte Ausführungsplattform auf Servern und Webhosts. Es liegt also der Schluss nahe, dass die Schaddaten nicht ausgeführt werden, wenn sie auf einen lokalen Endpunkt heruntergeladen werden.

Interessant ist jedoch, dass es mehrere Frameworks zur Anwendungsentwicklung gibt, die eine lokale NodeJS-Bereitstellung nutzen.[9] Auch wenn die Mehrheit der auf diesen Plattformen erstellten Finanzanwendungen auf Kryptowährungen ausgerichtet sind, gibt es verschiedene Open Source- und Freeware-Anwendungen für Börsenbenachrichtigungen, Finanzdatenanalysen und offene Handelsplattformen (die meist von den ins Visier genommenen Maklerfirmen verwendet werden).[10]

Kapitalmärkte: Bedrohungsanalyse und Trends

Finanzbeteiligungen sind die am stärksten betroffene Branche mit 31 % der Nachrichten und 23 % der Kunden. Hier gibt es einige Überschneidungen mit den Handelsbanken.

Über einen Zeitraum von sechs Monaten (vom 4. Quartal 2019 bis zum 2. Quartal 2020) hat Proofpoint Threat Intelligence die folgenden Bedrohungen beobachtet, die sich konsequent gegen Kapitalmärkte richten (siehe Abb. 2).

[8] Accenture (2020); „The State of Cybercrime in Banking and Capital Markets“ (Der Stand bei Cyberkriminalität bei Banken und Kapitalmärkten).

[9] https://brainhub.eu/blog/javascript-frameworks-for-desktop-apps/

[10] https://www.electronjs.org/apps?category=finance

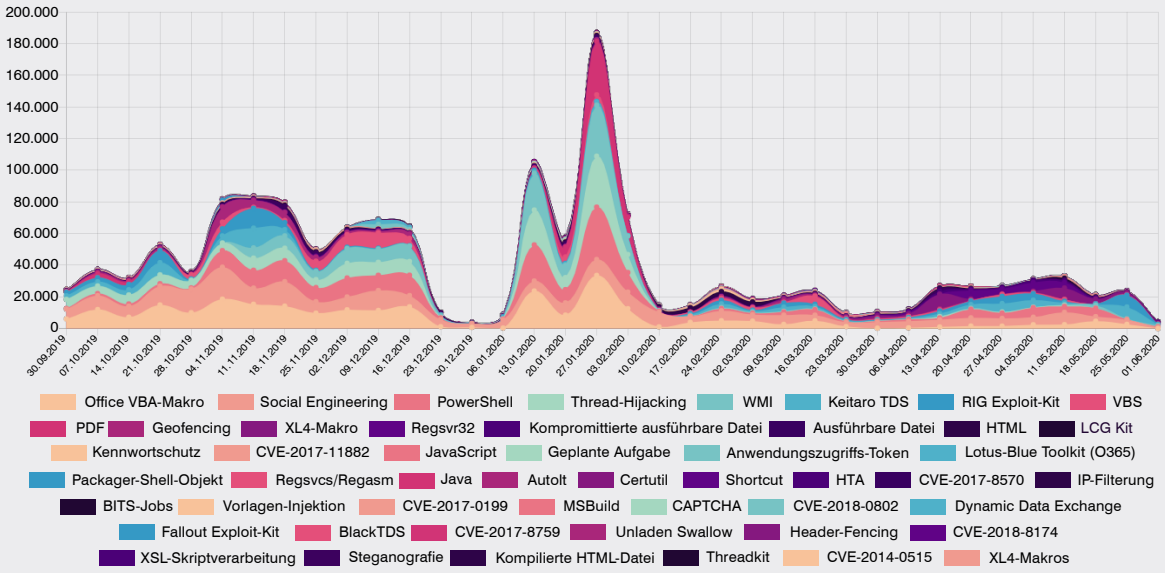


Abb. 2: Wertpapierhandel – Gezielte Exploits (Quelle: Proofpoint).

Regionaler Angriffstrend

Analystenkommentar: Bei der Untersuchung der 20 wichtigsten globalen Investmentbanken mit Hauptsitz in den USA kam heraus, dass die Top 50 der VAPs in fast jedem Unternehmen in Singapur, China oder Japan ansässig waren – obwohl man einen Großteil der Mitarbeiter in London oder New York vermuten würde.

Dies liegt möglicherweise an der Zunahme der APAC-basierten Neueinstellungen, die speziell den neueren Investmentinteressen in den APAC-Ländern Rechnung tragen sollen. „Banker sind der Auffassung, dass chinesische Unternehmen in staatlichem Besitz im Jahr 2020 für Abschlüsse eine wichtige Rolle spielen werden und erwarten eine hohe Beteiligung ..., um die Aktivität auf den Kapitalmärkten über Wasser zu halten."[11]

Sonstige Kampagnen

QuasarRAT | HTML | „Hinweise zur IRS-Korrespondenz"

E-Mails mit dem Betreff „Hinweise zur IRS-Korrespondenz" enthalten einen ZIP-gepackten HTML-Anhang. Beim Öffnen wird ein eingebettetes Word-Dokument abgelegt, das Makros zum Herunterladen eines VBscript verwendet, welches wiederum QuasarRAT herunterlädt. Kapitalmärkte (Investments und Wertpapiere) waren das einzige Ziel dieser Kampagne.

Versicherungen

Versicherungen werden der Finanzdienstleistungsbranche zugerechnet, da sie auf der Treuhandverwaltung von Fonds basieren, die im Versicherungsfall verfügbar gemacht werden müssen. Die Versicherungsbranche unterscheidet sich jedoch von den anderen Marktsegmenten, da sich die Hauptrisiken aus externen Ereignissen ergeben.

Angesichts der Vielzahl potenzieller schädlicher Zielsetzungen kommt es nicht nur darauf an, festzustellen, wer in Ihrem Unternehmen Zielscheibe sein könnte, sondern auch warum.

ÜBERSICHT: BESONDERHEITEN FÜR DEN SEKTOR VERSICHERUNGEN

VAPs:	**Breit angelegtes Phishing**: • Technologieteam • Führungsebene • Personalabteilung/Personalvermittler **Gezielte BEC-Angriffe:** • Versicherungsmakler/Account Manager • Programmmanager (Pensionspläne, Gruppenleistungen usw.)

Aus einem Bericht von Proofpoint Threat Intelligence geht außerdem hervor, dass der Bereich Versicherungen mehr unerlaubte Cloud-Mandantenanmeldungen verzeichnet als Banken und Kapitalmärkte.

Ursache hierfür ist möglicherweise die Tatsache, dass Versicherungsunternehmen häufiger Big Data und KI-Technologien verwenden[12], was sich nur bei einer Cloud-Bereitstellung als kosteneffizient erweist.[13] Weitere Gründe können die kontinuierliche Kostenoptimierung von Abläufen durch die Nutzung robotergestützter Prozessautomatisierung (RPA), das Auslagern standardisierter Abläufe oder Verlagern von Daten und Abläufen in die Cloud sein.[14]

[11] Chatterjee, Murdoch (2020): „Exclusive: Bank of America to hire 50 bankers for Asia dealmaking team in 2020 – sources" (Bank of America will 2020 50 Bankexperten für ein Investment-Banking-Team in Asien einstellen), Reuters.

[12] Oliver (2019): „Insurance sector prepares for disruption" (Versicherungssektor bereitet sich auf Veränderungen vor), Financial Times.

[13] Thomson (2020): „Are Insurers' Confidence in their Cyber Defense Exposing Them to Revenue Losses?" (Kann das Vertrauen von Versicherern in ihre Cyberabwehr zu Umsatzverlusten führen?), Accenture.

[14] Deloitte (2020): „Deloitte Insights – 2020 Insurance Outlook" (Prognose für Versicherungen 2020).

Versicherungen: Gezielte Angriffe

Proofpoint Threat Intelligence hat Angriffe identifiziert, die sich gegen eine einzelne Rolle oder Firma richten. Das deutet auf ein klar definiertes Ziel hin, das durch firmenspezifische Erkundungen ausfindig gemacht wurde.

Das TrickBot-Ökosystem

Analystenkommentar: Allgemein gilt: Je breiter eine Kampagne in Bezug auf Nachrichtenvolumen und Empfänger angelegt ist, desto unwahrscheinlicher ist es, dass es sich um eine gezielte Kampagne handelt. Im Versicherungssektor wurden einige sehr hohe Konzentrationen von Kundengruppierungen innerhalb einer einzigen Kampagne festgestellt.

In diesem Fall gehörten 21 von 26 (81 %) der Empfängerorganisationen einer Versicherung an und 96 % aller Nachrichten wurden an den Versicherungskunden gesendet. Der Großteil der Nachrichten wurde an ein bestimmtes Versicherungsunternehmen gesendet. Es ist jedoch kein Zufall, dass weitere 25 Kunden, die weniger Nachrichten erhielten, derselben Branche angehörten. In der Regel ist die Verteilung an die Empfängerbranchen vielseitiger. Jedoch sind Versicherungen in rund 10 % bis 13 % der Fälle mit von der Partie, während die größte Zielbranche nur etwa 16 % bis 18 % der Nachrichten erhält.

Die Malware-Schaddaten selbst gehören zu den bekanntesten Bank-Trojanern, dessen Betreiber ein Botnet mit Affiliate-Modell nutzen. Die Standardisierung der TTPs wird deutlich, wenn wir die Funktionsweise dieser Bedrohung näher betrachten. Ein Bedrohungsakteur wird Kunde der TrickBot-Betreiber. Ihm wird ein Unterscheidungsmerkmal in Form eines „Gruppen-Tags“ zugewiesen, in diesem Fall „yas24“. Der dreistellige Code ordnet die Infizierung einer konkreten Kampagne/Untergruppe/Affiliate zu. Die Zahl ist meist iterativ, da die Gruppe weiterhin Malware verteilt.

Versicherungen: Bedrohungsanalyse und Trends

Über einen Zeitraum von sechs Monaten (vom 4. Quartal 2019 bis zum 2. Quartal 2020) hat Proofpoint Threat Intelligence die Bedrohungen verfolgt, die sich konsequent gegen Versicherungen richten (siehe Abb. 3).

AZORult | „daffy“

E-Mails mit dem Betreff „Mail Report From support@WellsFargo.com“ enthalten einen Microsoft Word-Anhang mit dem Namen „purchase order nl5753637.doc“, der CVE-2017-8570 ausnutzt. Beim Öffnen des Anhangs wird AZORult (auch bekannt unter „daffy.exe“) heruntergeladen und ausgeführt. Obwohl die Versicherungsbranche nur 18 % der Kunden ausmacht, erhält sie 85 % der Nachrichten.

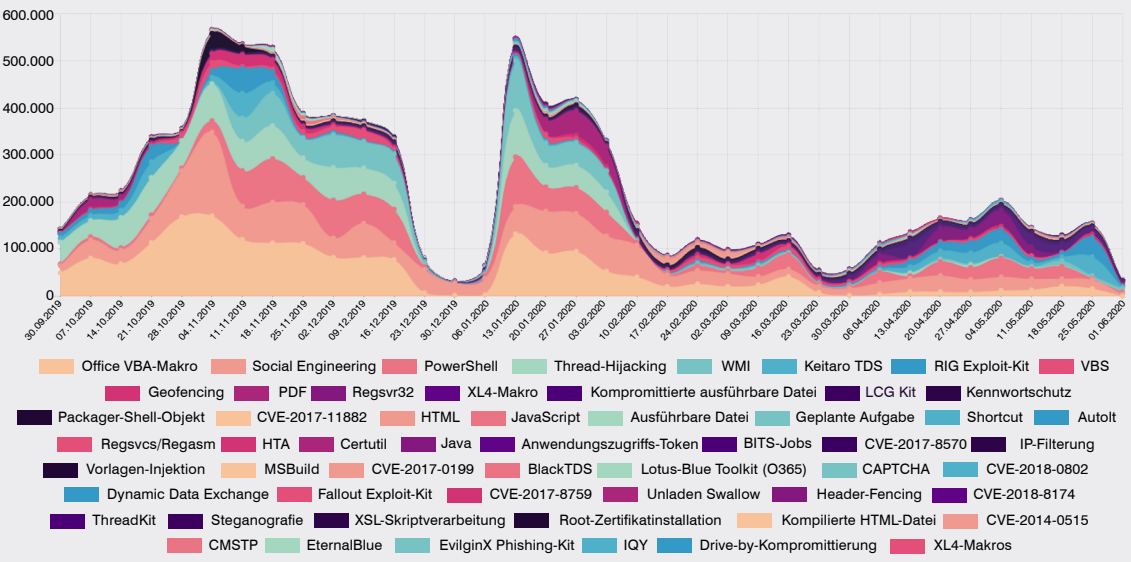


Abb. 3: Versicherungen – Gezielte Exploits (Quelle: Proofpoint).

Schlussfolgerungen und Empfehlungen

Cybersicherheit bei Finanzdienstleistern und Versicherern darf sich nicht nur auf externe Angriffsflächen konzentrieren, sondern muss auch Sicherheitslücken berücksichtigen, die durch interne Prozess- und Technologie-Optimierungen entstehen. Heutige Angriffe richten sich nicht mehr ausschließlich gegen Technologie, sondern auch gegen Menschen. Sie nutzen den „Faktor Mensch" bei modernen Anbietern aus: den Wunsch, Kunden beim Erreichen ihrer Ziele zu unterstützen und ihnen Chancen zu bieten. Die weltweite Pandemie hat viele Unternehmen aus dem Bereich Finanzdienstleistungen und Versicherungen dazu veranlasst, die Digitalisierung zu beschleunigen, um das Omnichannel Relationship Management für Kunden, den Service für Lösungen und den Vertrieb zu verbessern. Der Spagat zwischen zusätzlicher Sicherheit und Effizienz für die Mitarbeiter im Home Office und Informationssicherheit und -Compliance war noch nie so schwierig – und so wichtig. Aktuelle Bedrohungen und Compliance-Risiken für Finanzdienstleister und Versicherungsunternehmen können nur mit einem auf den Mensch ausgerichteten Schutz abgewehrt werden.

Für diese Unternehmen haben wir folgende Empfehlungen:

- **Setzen Sie auf einen personenzentrierten Sicherheitsansatz.** Angreifer sehen die Welt nicht als Netzwerkdiagramm, sondern suchen sich ihre Opfer gezielt aus. Verwenden Sie eine Lösung, die Ihnen zeigt, wer in Ihrem Unternehmen wie angegriffen wird und ob die angegriffene Person auf einen schädlichen Link geklickt hat. Berücksichtigen Sie dabei das individuelle Risiko der einzelnen Anwender. Mit einer personenzentrierten Lösung erfahren Sie, wie sie angegriffen werden, auf welche Daten sie zugreifen können und wie leicht sie sich täuschen lassen.
- **Verwenden Sie die Daten Ihres personenzentrierten Programms, um das erforderliche Budget für Ihre Sicherheitsprogramme zu definieren.** Anhand dieser Daten können Sie gegenüber der Geschäftsführung Ihre Prioritäten erläutern und zeigen, wie die Programme die Risiken für das Unternehmen reduzieren. Außerdem können Sie mithilfe dieser Daten Mitarbeitern in allen Unternehmensbereichen zeigen, warum Ihr Programm wichtig ist und wie sie sich selbst und das Unternehmen schützen können.
- **Schulen Sie Ihre Anwender darin, schädliche E-Mails zu erkennen und zu melden.** Regelmäßige Schulungen und simulierte Angriffe können Risiken auf zweierlei Weise verringern: Ihre Anwender erfahren, wie sie viele Angriffe stoppen können. Gleichzeitig erfahren Sie, welche Anwender möglicherweise besonders gefährdet sind. Die besten Simulationen imitieren reale Angriffstechniken. Ziehen Sie Lösungen in Betracht, die aktuelle Angriffstrends im Bereich Finanzdienstleistungen und Versicherungen sowie die neuesten Bedrohungsdaten berücksichtigen. Wenn Anwender verdächtige E-Mails melden, kann Automatisierung helfen, die tatsächlichen Bedrohungen zu verifizieren und zu beheben.
- **Gehen Sie davon aus, dass Anwender früher oder später auf einen Link klicken werden.** Angreifer finden immer neue Möglichkeiten, den Faktor Mensch auszunutzen. Suchen Sie nach einer Lösung, die bei Ihren Anwendern eingehende E-Mail-Bedrohungen erkennt und blockiert – bevor sie den Posteingang erreichen. Stoppen Sie externe Bedrohungen, die Kunden mithilfe Ihrer Domäne angreifen. Mit effektivem Schutz vor Datenverlust über E-Mails (DLP) bleiben Ihre Daten sicher und verfügbar. Suchen Sie nach einer Lösung, die vertrauliche und kritische Informationen zuverlässig klassifiziert und gewährleistet, dass nur die richtigen Personen darauf zugreifen können.
- **Errichten Sie eine zuverlässige Abwehr zum Schutz vor Business Email Compromise (BEC, auch als Chefmasche bekannt).** E-Mails mit gefälschter Identität lassen sich mit herkömmlichen Sicherheitstools mitunter nur schwer erkennen. Investieren Sie daher in eine Lösung, die E-Mails basierend auf benutzerdefinierten Quarantäne- und Blockierungsrichtlinien verwaltet. Ihre Lösung sollte externe ebenso wie interne E-Mails analysieren, da Angreifer möglicherweise kompromittierte Konten missbrauchen, um Anwender in Ihrem Unternehmen zu täuschen. Implementieren Sie E-Mail-Authentifizierung per DMARC (Domain-Based Message Authentication, Reporting and Conformance), um Spoofing-E-Mails zu stoppen, bevor sie Ihre Angestellten und externe Geschäftspartner erreichen.
- **Setzen Sie bei Fernzugriffen auf das Prinzip „Vertrauen ist gut, Kontrolle ist besser" – kurz: Zero Trust.** Finanzdienstleister und Versicherer speichern und verarbeiten heute mehr Daten als je zuvor, müssen eine größere digitale Umgebung verwalten und arbeiten mit einer stark verteilten Belegschaft. All das bietet Cyberkriminellen neue Angriffsflächen. Gleichzeitig kann herkömmliche VPN-Technologie mit der Entwicklung nicht Schritt halten. Investieren Sie in eine Zero-Trust-Lösung, die Mitarbeiter, externe Geschäftspartner und Kunden schnell und sicher mit Ihrem Rechenzentrum und der Cloud verbinden kann.
- **Isolieren Sie riskante Websites und URLs.** Halten Sie riskante Webinhalte von Ihrer Umgebung fern, indem Sie verdächtige Webseiten und nicht verifizierte URLs in einem geschützten Container innerhalb des normalen Webbrowsers des Anwenders darstellen lassen. Diese Web-Isolierungstechnologie ist ein wichtiger Schutz für E-Mail-Konten, die von mehreren Personen genutzt werden und daher nur schwer mit Multifaktor-Authentifizierung abgesichert werden können. Außerdem können Sie auf diese Weise das private Surfverhalten sowie die Webmail-Services Ihrer Anwender isolieren und die Freiheit und Privatsphäre Ihrer Mitarbeiter gewährleisten, ohne das Unternehmen zu gefährden.

- **Schützen Sie Microsoft 365 und andere Cloud-Anwendungen.** Je mehr Finanz- und Versicherungsdaten und -anwendungen in die Cloud wechseln, desto mehr Einblick in die Cloud-Aktivitäten benötigen Sie. Ein Cloud Access Security Broker (CASB) ermöglicht schnelle Prüfungen und umgehende Reaktionen auf potenzielle Richtlinienverletzungen in Cloud-basierten E-Mails in allen Service-Bereichen.
- **Identifizieren und stoppen Sie Bedrohungen durch Insider.** Schützen Sie Ihr Unternehmen vor Datenverlust, Sabotage und Markenschädigung, die durch böswillig oder fahrlässig handelnde oder kompromittierte Insider entstehen. Implementieren Sie eine Lösung zur Abwehr von Insider-Bedrohungen, die Aktivitäten und Datenbewegungen korreliert, damit Sie die Zusammenhänge zwischen Anwenderverhalten und Absichten erkennen. Unterstützen Sie Ihre Sicherheitsteams bei der Identifizierung von Anwenderrisiken, bei der Erkennung und Behebung von Datenschutzverletzungen durch Insider sowie bei der Beschleunigung von Reaktionen auf Sicherheitszwischenfälle.
- **Minimieren Sie Ihre Compliance-Risiken.** Die Compliance-Bestimmungen für die Finanzdienstleistungs- und Versicherungsbranche unterliegen einer kontinuierlichen Entwicklung. Die Zahl der Audits wächst ebenso wie die Höhe der Geldstrafen und die juristischen Probleme im Zusammenhang mit externen Geschäftspartnern. Suchen Sie daher nach einer Archivierungs- und Compliance-Lösung, die Datenlecks durch böswillig und fahrlässig handelnde Insider schnell erkennen und schließen kann. Identifizieren und stoppen Sie zudem betrügerische Geschäftspraktiken wie Rechnungsbetrug und Bestechungsgelder.
- **Arbeiten Sie mit einem Anbieter für Bedrohungsdaten zusammen.** Für kleinere, gezielte Angriffe benötigen Sie erweiterte Bedrohungsinformationen. Implementieren Sie eine Lösung, die mithilfe von statischen und dynamischen Techniken Angriffs-Tools, -Taktiken und -Ziele aufdeckt und daraus Erkenntnisse zieht.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0400-003-01-01 1/21