CYBER THREAT REPORT
EDITION 2021/22

Die Welt der Cyberkriminalität steht nicht still! Im neuen **Cyber Threat Report** - Edition 2021/22 werfen die IT-Experten von Hornetsecurity daher wieder einen genauen Blick auf das Einfallstor E-Mail-Kommunikation und analysieren die neuesten Maschen der Cyberkriminellen. Dabei untersuchen sie, welche Gefahren 2021 aufgetaucht sind, was aus Emotet geworden ist und worauf sich Unternehmen beim Öffnen ihres Postfachs zukünftig gefasst machen müssen.

Mit den inhouse entwickelten Services wie Spam and Malware Protection, Advanced Threat Protection sowie der vollumfänglichen Security Suite für Microsoft 365 schützt der E-Mail-Cloud-Security- und Back-up-Provider Hornetsecurity mittlerweile über 50.000 Kunden weltweit. Zugleich können die Security Analysten auf Grundlage ausgewerteter Filter-Daten und ihres Know-hows fundierte Aussagen zur derzeitigen Bedrohungslage durch Cybercrime treffen.

Kapitel 1: Cyberkriminalität gehört zu den größten Bedrohungen weltweit

Laut des neuesten Reports "Hidden Costs of Cybercrime" des US-amerikanischen Herstellers für Computersicherheit McAfee, lagen die finanziellen Verluste durch Cyberkriminalität im Jahr 2020 weltweit bei **945 Milliarden US-Dollar**[1]. In 2018 beliefen sich die monetären Schäden noch auf rund 600 Milliarden US-Dollar[1] - Innerhalb von zwei Jahren hat sich dieser Betrag weiter dramatisch erhöht. Diese finanziellen Schäden umfassen unter anderem **Opportunitätskosten, System- und Produktivitätsausfall sowie Markenschädigung.**

Die Sicherheit und der reibungslose Ablauf von IT-Prozessen nehmen mittlerweile einen so hohen Stellenwert im gesellschaftlichen sowie ökonomischen Leben ein, dass das World Economic Forum in seinem Global Risk Report 2021 das Versagen von Cyber-Sicherheitsinfrastruktur und -Maßnahmen in Unternehmen, Regierungen sowie auch privaten Haushalten in die Liste der derzeit aktuellen sowie auch mittelfristig kritischsten Bedrohungen für die Welt einordnet. Denn das Erliegen der IT-Security könnte zu enormen Einschränkungen des wirtschaftlichen Geschehens, finanziellen Verlusten sowie geopolitischen Spannungen führen und stellt damit auch ein hohes Risiko für die Stabilität des gesellschaftlichen Lebens dar.[2]

Insgesamt erkennen immer mehr Unternehmen das mögliche Ausmaß, welches ein Cyberangriff mit sich bringt und das wachsende Risiko, Opfer einer Cyberattacke zu werden. Dies zeigt sich in den **steigenden Investitionen von Unternehmen in ihre IT-Sicherheit: In 2020 beliefen sich die weltweiten Ausgaben für Cyber-Sicherheit auf rund 133,8 Milliarden US-Dollar.** Für das Jahr 2021 werden die Ausgaben auf etwa 150 Milliarden US-Dollar geschätzt.[3]

Die E-Mail gilt weiterhin als eines der Haupteinfallstore für Cyberangriffe in Unternehmen, Organisationen sowie Regierungseinrichtungen. Business Email Compromise sowie Ransomware stellen dabei die gefährlichsten Angriffsarten dar, bei denen die Hacker von Jahr zu Jahr trickreichere Vorgehensweisen anwenden, um ihre Ziele zu erreichen. Doch auch Datendiebstahl und -Spionage und die Installation von Backdoors sind für Behörden und Wirtschaft eine ernstzunehmende Bedrohung.

Kapitel 2: Email Threat Review 2021 des Security Labs

Die Threat Researcher des Hornetsecurity Security Labs geben im Folgenden einen Einblick in die Kennzahlen zur derzeitigen Lage der weltweiten E-Mail-Bedrohungen. Die Experten werteten im bisherigen Jahr 2021 eingegangene E-Mails aus und klassifizierten diese.

Spam, Threats und Advanced Threats: Die unbemerkten Gefahren im E-Mail-Verkehr

Etwa 300 Milliarden E-Mails werden tagtäglich versendet – laut Prognose soll die Zahl der privat und geschäftlich versendeten sowie empfangenen E-Mails bis 2024 sogar auf 361,6 Milliarden ansteigen.[4]

Die E-Mail stellt also weiterhin das Hauptkommunikationsmittel für Unternehmen dar, über das nicht nur sensible Informationen, sondern auch unternehmensinterne Dateien ausgetauscht werden.

Die Experten vom Hornetsecurity Security Lab haben den E-Mail-Verkehr des ersten Halbjahrs 2021 analysiert und konnten feststellen, dass insgesamt **60 % der bei Hornetsecurity eingegangenen E-Mails als "clean"**, also erwünscht, klassifiziert werden konnten. Diese tragen zum produktiven Austausch sowie normalen Betriebsablauf bei. Jedoch wurden **40 % der eingegangenen E-Mails entsprechend als "unerwünscht" eingestuft.**

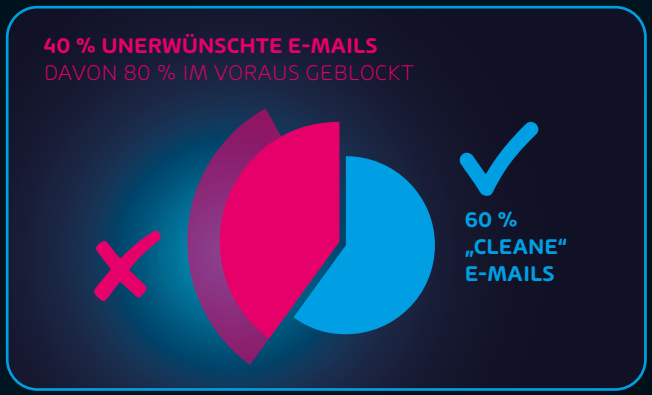


Abb. 1: Klassifikation der von Hornetsecurity gescannten E-Mails

Von den unerwünschten E-Mails wurden **rund 80% bereits im Voraus abgewiesen:** Dazu zählen unter anderem E-Mails, die mithilfe einer Real-time Blackhole List als Spam klassifiziert wurden, Nachrichten, die versuchten die Hornetsecurity Mailserver als Open Relay zu verwenden sowie technische Fehler, Greylisting oder nicht identifizierbare E-Mail-Adressen.

Das Security Lab klassifizierte 15,54 % aller unerwünschten E-Mails als Spam, 4 % als Threats und 1 % wurde von Hornetsecuritys Advanced Threat Protection erkannt und stellt "fortschrittliche Bedrohungen" dar. Dazu zählen CEO-Fraud, Spear Phishing oder Angriffe mit neuartiger, teilweise noch unbekannter Malware.

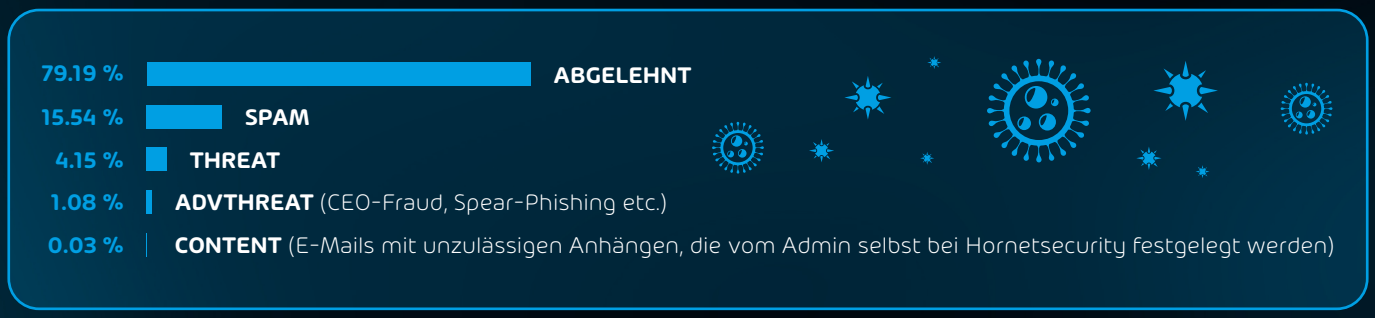


Abb. 2: Anteil unerwünschter E-Mails nach Kategorie

Anhänge in schädlichen E-Mails

Um nicht von den Spam- und Virenfiltern ihrer Opfer entdeckt zu werden, verbergen Cyberkriminelle Malware auf verschiedene Art und Weise in ihren E-Mail-Attacken. In 2021 galten Archivdateien mit 33,6 % als beliebtestes Vorgehen, um Schadsoftware zu verbreiten. Die ausführbare Malware bzw. das mit Malware infizierte Dokument wird dabei komprimiert und direkt an die Angriffs-E-Mail angehängt. Die Hoffnung dabei ist, dass das Ziel-E-Mail-System nicht in der Lage ist, komprimierte Anhänge zu scannen. Kriminelle Akteure mit weniger "Erfahrung" nutzen diese Technik häufig, da sie keine technischen Kenntnisse erfordert.

In 15,3 % der Fälle verwendeten Cyberkriminelle HTML-Dateien in ihren Angriffs-E-Mails. In einer Phishing-Mail wird die Phishing-Website als HTML direkt an die E-Mail angehängt, wodurch URL-Filter umgangen und die Opfer auf die schädlichen Websites zum Download

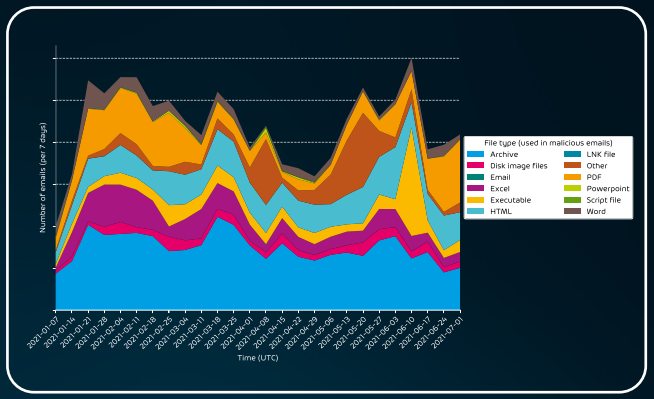


Abb. 4: Verteilung schädlicher E-Mail-Anhänge pro Woche (im 1.Halbjahr 2021)

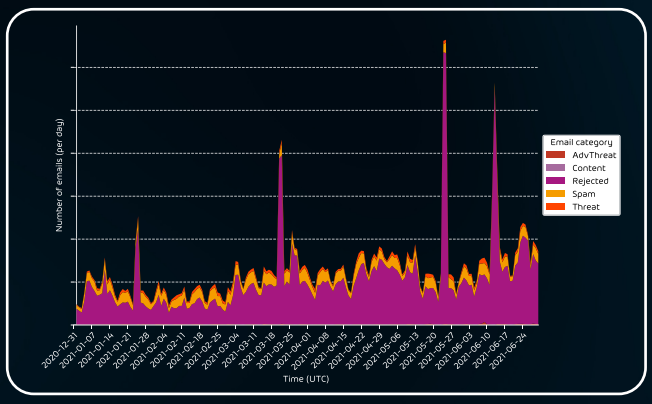


Abb. 3: Verteilung unerwünschter E-Mails nach Kategorie im ersten Halbjahr 2021

der Malware verleitet werden sollen. Es wird also keine anklickbare URL in der E-Mail eingefügt.

Excel-Dateien (.xls, .xlsm, .xlsx, .xslb usw.) mit XLM-Makros wurden im vergangenen Jahr immer beliebter (10,2 % im 1. Halbjahr 2021). Im Gegensatz zu VBA-Makro-Malware wird XLM-Makro-Malware seltener erkannt und daher von vielen Bedrohungsakteuren bevorzugt. Tatsächlich verwendeten zahlreiche Cyberkriminelle denselben bösartigen Dokumentengenerator namens „EtterSilent", um ihre XLM-Makro-Dokumente zu erzeugen.

Weitere zur Kompromittierung genutzte Datei-Typen sind PDF (14,5 %), Word (4,8 %) sowie PowerPoint (0,4 %) – PDF-Dateien werden vor allem für die Verbreitung schädlicher Links verwendet. Excel, PowerPoint und Word enthalten oftmals Makros.

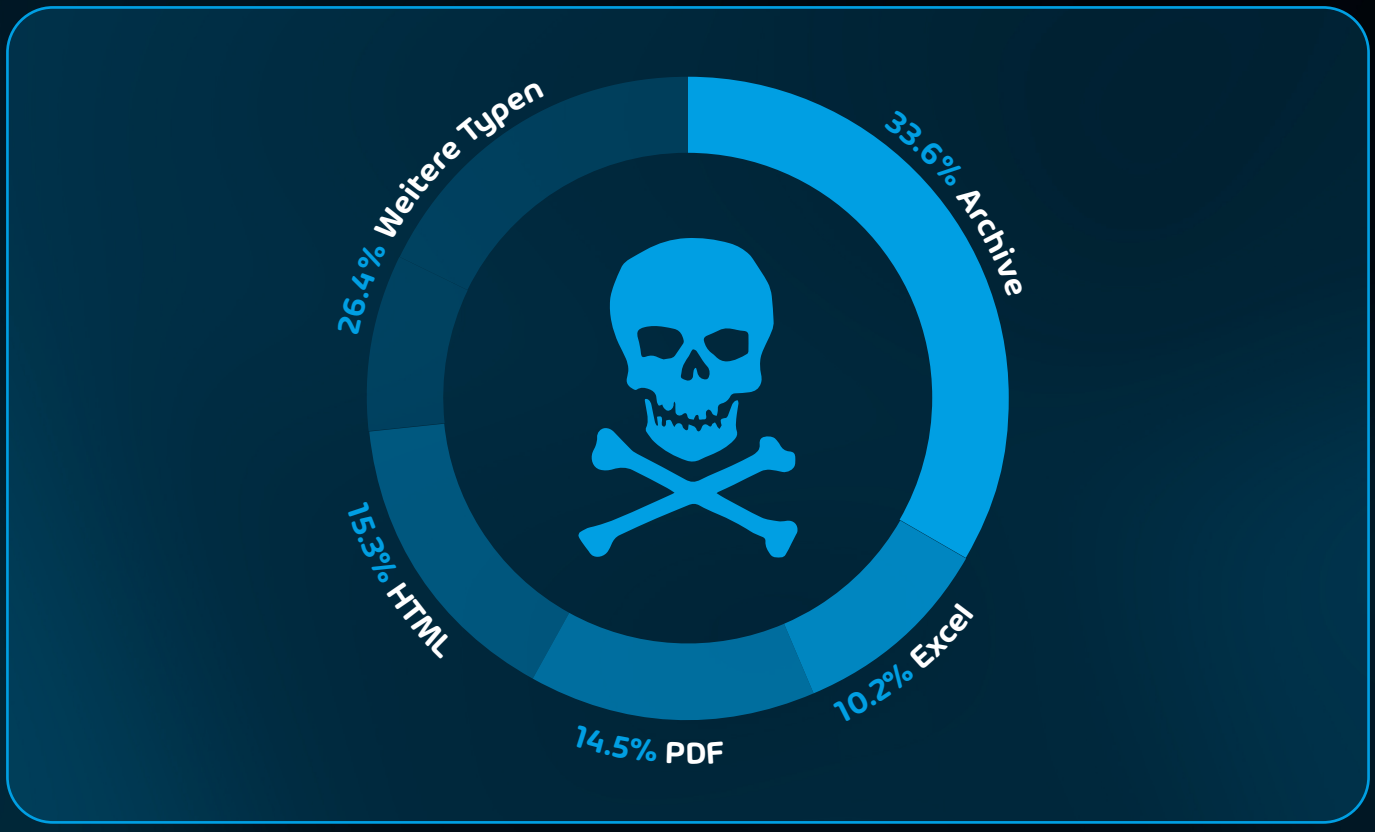


Abb. 5: Meistgenutzte Datei-Typen in schädlichen E-Mails

Industry Threat Index: Diese Branchen sind aktuell besonders betroffen

In den meisten Fällen wird eine schädliche E-Mail an eine Vielzahl von E-Mail-Adressen versendet. Dennoch sind manche Unternehmen und Branchen von besonderem Interesse für Cyberkriminelle, weil sie beispielsweise davon ausgehen, dass zugehörige Unternehmen besonders hohen Umsatz generieren oder äußerst sensible und wertvolle Daten vorliegen haben. Die Security Lab Experten ermitteln mit dem Threat Index die Angriffsrate für unterschiedliche Branchen. Im ersten Halbjahr 2021 waren vor allem die Fertigungsbranche, Forschungs- und Entwicklungseinrichtungen sowie Firmen des öffentlichen Transportwesens, wie beispielsweise Bus und Bahn, Fluglinien sowie Taxiunternehmen von Cyberattacken betroffen.

- 4.9 | **FERTIGUNGSBRANCHE**
- 4.8 | **FORSCHUNG**
- 4.7 | **TRANSPORTWESEN**
- 4.6 | **BILDUNG**
- 4.6 | **MEDIEN**
- 4.5 | **AUTOMOTIVE**
- 4.5 | **UNTERHALTUNGSBRANCHE**
- 4.2 | **HOTELGEWERBE**
- 4.1 | **AGRARINDUSTRIE**
- 4.1 | **GESUNDHEITSWESEN**

Anteil der Threat E-Mails
(in Relation zu gültigen/cleanen E-Mails)*

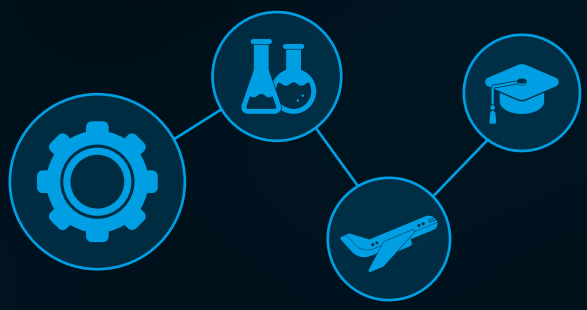
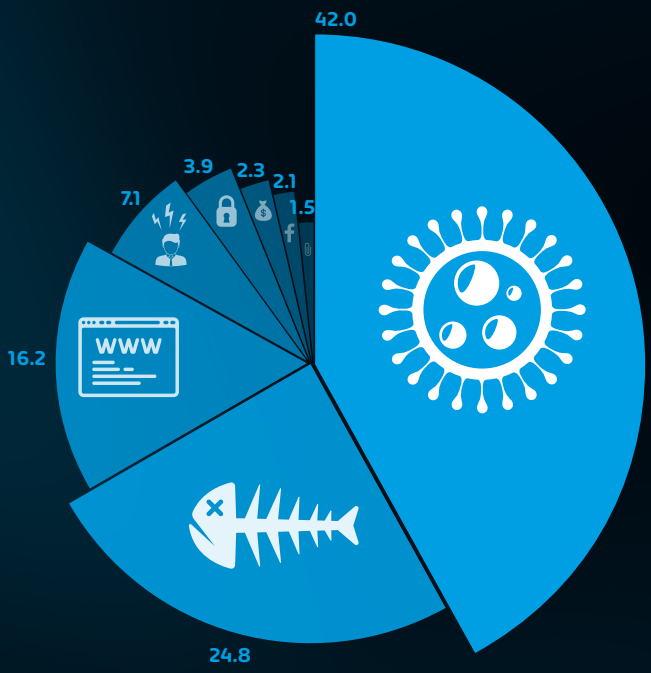


Abb. 6: Am stärksten bedrohte Branchen laut Threat-Index*

*Threat Index % = Anzahl schädliche E-Mails / (Anzahl schädliche E-Mails + Anzahl Clean E-Mails) * 100 – Ohne Spam und Infomails

Vorgehensweisen der Hacker in 2021

Um die Viren- und Spamfiltern zu umgehen, variieren Hacker die Inhalte und die Aufmachung ihrer Schad-E-Mails. Phishing, Brand Impersonation und Ransomware sind nur einige der Angriffstaktiken, um unerkannt und schließlich auch „erfolgreich" ins Postfach ihrer Opfer zu gelangen. **Phishing-E-Mails sind und bleiben wohl auch weiterhin eine der beliebtesten Angriffstaktiken:** Mit dieser Methodik versuchen Hacker an die verschiedensten Arten sensibler Daten zu gelangen – von Zugangsdaten bis hin zu Kreditkarteninformationen. Mit 7,1 % ist auch die „Erpressung" äußerst populär unter den Cyberkriminellen. Der sogenannte „Evergreen" hierbei sind die „Sextortion" -E-Mails: Das Opfer erhält eine E-Mail, in der behauptet wird, dass dessen Computer während des Besuchs einer pornografischen Website kompromittiert und ein Video aufgenommen wurde. Um zu verhindern, dass das Video an die Öffentlichkeit gelangt, soll ein Lösegeld gezahlt werden.



ANGRIFFSTAKTIK	%
Andere	42.0
Phishing	24.8
URL	16.2
Erpressung	7.1
Executable in archive/disk-image	3.9
Advance-fee scam (Vorschussbetrug)	2.3
Brand Impersonation	2.1
Maldoc (schädlicher Anhang)	1.5

Abb. 8: Die beliebtesten Angriffstaktiken im 1. Halbjahr 2021

Amazon oder Amaz0n? Vorsicht vor "Brand Impersonation"

Cyberangriffe, bei denen gezielt Unternehmen imitiert werden, sind auch bekannt als **„Brand Impersonation"**. Hierbei kopieren Cyberkriminelle das Corporate Design der imitierten Firma und benennen die Absenderadresse so, dass sie von der originalen E-Mail-Adresse kaum zu unterscheiden ist. In der Regel ist das Ziel dahinter, Zugangsdaten zu Nutzerkonten oder Kreditkartendaten abzugreifen, aber auch den Empfänger zum Klick auf einen schädlichen Link zu verleiten um beispielsweise unbemerkt Schadsoftware downzuloaden.

Amazon liegt in der Statistik der Experten vom Hornetsecurity Security Lab mit 17,7 % auf Platz 1 der meistkopierten Unternehmen. Auch DHL ist beliebt unter Cyberkriminellen: Besonders zu Corona-Zeiten ist die Anzahl an (Online-)Bestellungen jeglicher Waren in die Höhe geschossen – dementsprechend viele Pakete wurden verschickt und empfangen. Vor allem E-Mails, die die Ankunft eines Pakets ankündigen, sind für Cyberkriminelle leicht zu fälschen. Die E-Mail-Nachricht ist kurzgehalten, der Empfänger hinterfragt in den meisten Fällen die Herkunft nicht, wenn tatsächlich ein Paket erwartet wird und klickt auf den Sendungsverfolgungs-Link – dieser führt schließlich jedoch zum Download eines Schadprogramms oder auf eine Phishing-Website, so wie auf der folgenden Abbildung zu sehen:

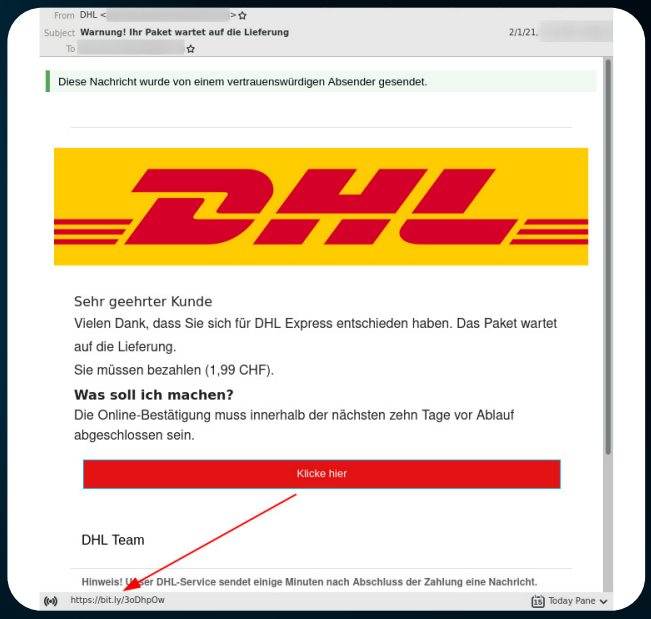


Abb. 9: Beispiel-E-Mail zu Brand Impersonation mit schädlicher URL

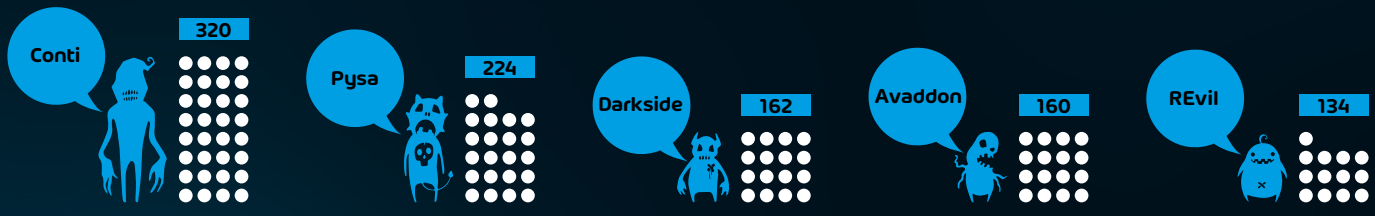
NACHGEAHMTE MARKE/ORGANISATION

- 17.7 | AMAZON
- 17.1 | ANDERE
- 16.5 | DEUTSCHE POST / DHL
- 12.7 | DOCUSIGN
- 5.7 | PAYPAL
- 3.5 | LINKEDIN
- 3.0 | MICROSOFT
- 2.5 | 1&1
- 2.3 | O2
- 2.2 | FACEBOOK
- 1.8 | HSBC
- 1.2 | FEDEX
- 1.1 | EBAY
- 1.1 | SANTANDER
- 1.0 | NETFLIX

Abb. 10: Genutzte Marken/Organisationen zum Einschleusen von Schadprogrammen oder Abfrage von Daten

Ransomleaks & Double Extortion: Trend nimmt größere Ausmaße an

Bereits im vergangenen Jahr prognostizierten die Hornetsecurity Threat Researcher einen Aufwärtstrend von Ransomware, die ihre Opfer zusätzlich durch Datenveröffentlichung erpresst. Diese Entwicklung verstärkte sich in den Folgemonaten. Bevor die Daten der mit Ransomware kompromittieren Rechner der Opfer verschlüsselt werden, kopieren die Angreifer die Dateien auf die Server, die dann mit der Veröffentlichung dieser sensiblen Informationen auf sogenannten Leak-Seiten drohen. Die Hackergruppe hinter der Conti-Ransomware ist mit veröffentlichten Daten von 320 Opfern am „fleißigsten". Die Threat Researcher vom Hornetsecurity Security Lab konnten außerdem Leaks auf folgenden Ransomware Leak Sites beobachten:



Und 23 weiteren: Babuk (70), Cl0p (52), Doppelpaymer (43), Nephilim (40), Lorenz (27), Ragnarok (22), Promethous (22), Everest (19), Xing Team (18), Astro Team (17), MountLocker (16), Grief (16), RansomEXX (16), Vice Society (14), RagnarLocker (11), Cuba (9), Networm (5), Egregor (5), Synack (4), LV (3), Hive (3), Suncrypt (3), Lockbit (2)

Abb. 11: Die größten Leaksites nach Opferanzahl (Anzahl der Personen, deren Daten auf jeweiliger Seite veröffentlicht wurden)

Gefahreneinstufung des Hornetsecurity Security Labs

Aufgrund der beobachteten Entwicklungen des "as a Service"-Markts im Darknet gehen die Security-Experten davon aus, dass zukünftig die steigende Cyberkriminalität zunehmend von hochprofessionell arbeitenden Cyberkriminellen ausgeht. Ransomware-as-a-Service ist hierbei weiterhin ein großes Thema und die Entwicklung dieser kriminellen Vorgehensweise stellt eine immer größere Bedrohung für Unternehmen, öffentliche Einrichtungen, wie beispielsweise Krankenhäuser, sowie Regierungen dar.

Insgesamt hat der Ransomware-Trend noch längst nicht seinen Höhepunkt erreicht. Die Ransomware-Gruppe REvil habe laut Bleeping-Computer 1 Milliarde US-Dollar in Bitcoin eingenommen – und das innerhalb eines Jahres.[5] Von dieser hohen Summe können Drahtzieher von Gruppen wie REvil zum Beispiel professionelle Penetrations Tester einstellen, die wiederum weitere Opfer auffindbar machen, deren Daten dann ebenfalls durch die Hacker-Gruppe angegriffen werden.

Kapitel 3: Die "Threat-Highlights" 2021

Das Jahr 2021 hielt ein paar aufsehenerregende Ereignisse im Zusammenhang mit Cyberkriminalität bereit, die wir im folgenden Kapitel noch einmal Revue passieren lassen.

Der Takedown von Emotet: Das Auf und Ab der gefährlichsten Schadsoftware der Welt

Der „gefährlichsten Schadsoftware der Welt" konnte endlich Einhalt geboten werden: Am Anfang des Jahres 2021 meldeten beteiligte Polizeieinheiten die Zerschlagung des Emotet-Botnets.

Emotet wurde erstmals im Jahr 2014 entdeckt: Damals handelte sich um einen Banking-Trojaner, der Bankdaten und Anmeldeinformationen stahl. Mit der Zeit entwickelte sich Emotet allerdings zu einem Malware-as-a-Service (MaaS)-Betrieb, der die Verteilung von Malware für andere Cyberkriminelle anbot. Emotet hat allein in Deutschland neben Computern von zehntausenden Privatpersonen auch eine hohe Anzahl von Business-IT-Systemen infiziert. Das Klinikum Fürth und das Kammergericht Berlin waren nur zwei von vielen Opfern Emotets. Allein in Deutschland schätzt das BKA die Schäden, die durch Emotet verursacht wurden, auf 14,5 Millionen Euro.

Nach einer erfolgreichen Systeminfektion konnte Emotet Kontaktbeziehungen sowie E-Mail-Inhalte in Postfächern auslesen. Um Malware zu verbreiten, antwortete Emotet auf Basis der gesammelten Informationen sehr authentisch auf diese E-Mails – die Fälschungen waren nur sehr schwer zu identifizieren. Diese Vorgehensweise ist auch als E-Mail-Konversations-Thread-Hijacking[6] bekannt. Hornetsecurity veröffentlichte bereits zahlreiche Blogposts über Emotet-Angriffe wie diese.

Am 27. Januar 2021 gab Europol bekannt, dass eine internationale, weltweite Operation von Strafverfolgungs- und Justizbehörden, unter anderem aus Deutschland, den Niederlanden, Litauen, der Ukraine, Frankreich, England sowie Kanada und den USA, die Infrastruktur von Emotet übernehmen und zerschlagen konnte.

Die Ermittler erhielten die Kontrolle über die Infrastruktur indem verschiedene Server identifiziert wurden, über die die Schadsoftware verteilt wurde. Schritt für Schritt konnten weite Teile der Infrastruktur aufgedeckt werden. So war es den Ermittlungsbehörden möglich, den Tätern den Zugriff darauf zu unterbinden, und von einem der verdächtigten Betreiber in der Ukraine sogar die Kontrolle zu übernehmen.

Die C2-Kommunikation von Emotet wurde gekappt und die Informationen der damit verbundenen Opfer an die zuständigen CERTs des Landes weitergegeben, die die Opfer benachrichtigt haben, damit sie die Schadsoftware entfernen können.

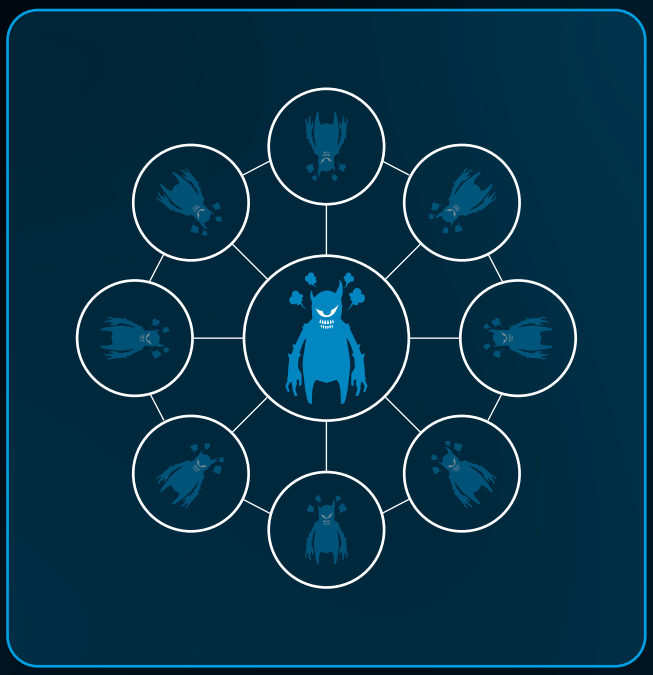
Bis zum Takedown, machte Emotet ganze 20% von den von Hornetsecurity analysierten schädlichen E-Mails aus. Am 15.11. registrierten die Threat Researcher von Hornetsecurity jedoch wieder erste Aktivitäten der Schadsoftware. Dabei wurde die TrickBot-Malware über Malspam verbreitet, heruntergeladen und installierte schließlich die Emotet-Malware. Anschließend wurde das Emotet-Botnet neu aufgebaut und begann erneut Malspam aus seinem Botnet zu versenden.

Emotet – The Aftermath

Mit dem Untergang von Emotet gibt es neue Anwärter, die den Platz des Botnets einnehmen wollen: Quakbot verfügt über die nötige Raffinesse, doch sein Botnet ist noch lange nicht so groß wie das von Emotet. Das macht die großflächige Verteilung der Malware schwieriger.

Andere, wie das Cutwail-Botnet mit seinem Dridex-Malspam oder die Akteure hinter den Hancitor-Malspam-Kampagnen, können Malspam zwar in großem Umfang verbreiten, verfügen jedoch nicht über die Gerissenheit von Emotet.

Es ist damit zu rechnen, dass noch weitere Akteure planen, den Titel "die gefährlichste Schadsoftware der Welt" zu ergattern, da der bestehende Kundenstamm von Emotets Malware-as-a-Service (MaaS)-Betrieb weiterhin existiert und das Vorgehen auch von anderer Malware genutzt werden könnte.[7]



Verhaftungen rund um Clop, The Trick & Gozi

Neben der Zerschlagung des Emotet-Botnets gab es in 2021 weitere gute Nachrichten: Unter anderem verhaftete die nationale Polizei der Ukraine einige Personen, die unter Verdacht standen, Unternehmen mit der Clop-Ransomware infiziert zu haben. Die Clop-Ransomware-Operation lief allerdings ohne Unterbrechung weiter, was den Threat Researchern aus dem Security Lab Anlass gibt zu glauben, dass die verhafteten Personen keine wichtigen Drahtzieher hinter der Ransomware waren.

Eine weitere verdächtigte Person, die seit 2013 gesucht wurde, da sie mit der Gozi-Malware in Verbindung gebracht werden konnte, wurde ebenfalls verhaftet. Der Verdächtigte betrieb einen Bulletproof-Host, der Cyberkriminellen dabei half, die Gozi-Malware, den Zeus-Trojaner und den SpyEye-Trojaner zu verbreiten. Außerdem wird der Verdächtigte beschuldigt, DDoS-Angriffe und Spam-Übertragungen initiiert zu haben.

Eine Mitentwicklerin der The Trick-Malware wurde ebenfalls in den USA verhaftet und in 19 von 47 Anklagepunkten angeklagt.[8]

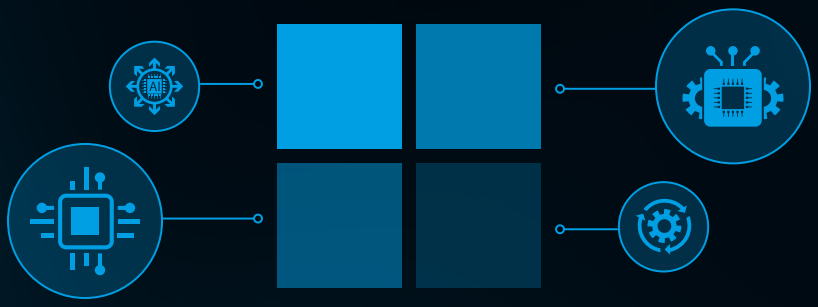
Der Microsoft Exchange Hack

Im März schloss Microsoft mit einem außerplanmäßigen Sicherheitsupdate vier Schwachstellen in unterschiedlichen Versionen der Microsoft Exchange Server. Doch nur kurze Zeit nach der Veröffentlichung begannen massenhafte Infektionen der ungepatchten Exchange-Server über das Internet.

Schätzungsweise 250.000 Server waren von den Angriffen betroffen. Selbst das Weiße Haus hat die Betroffenen aufgefordert, Sicherheits-Patches in ihren jeweiligen Exchange-Systemen zu installieren und das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Alarmstufe Rot ausgerufen, da die Behörde die Bedrohungslage zu dieser Zeit als extrem kritisch einschätzte.

Als Drahtzieher wird die chinesische Hackergruppe Hafnium vermutet, die staatlich gesponsert wird und für hoch qualifizierte und ausgeklügelte Angriffe bekannt sei.[9]

Im April 2021 schaltete sich sogar das FBI ein. Ein Gerichtsbeschluss gab dem FBI die Befugnis, in Unternehmensnetzwerke einzudringen, um von Infektionen zurückgelassene Webshells zu entfernen, die von Cyberkriminellen für weitere Angriffe genutzt werden konnten.[10]



Kapitel 4: Prognosen und mögliche Entwicklungen des Cybercrime

Die Digitalisierung und die zunehmende Vernetzung von Geräten und Accounts bietet Cyberkriminellen nicht nur mehr Platz für ihre Machenschaften – Cyberkriminalität ist über Grenzen und Kontinente hinweg mühelos möglich und somit schwer nachzuverfolgen. Auch laut dem Bundeskriminalamt verlagert sich die Kriminalität vermehrt in den digitalen Raum. Im Vergleich zum Vorjahr sind Straftaten über das Internet um 8,7 % gestiegen, besonders die Deliktsfelder der Cyberkriminalität weisen 2020 einen Anstieg von 7,9 % im Vergleich zum Jahr 2019 auf.[11]

In einer repräsentativen Studie des Digitalverbands Bitkom wurde deutlich, dass 75 % der befragten Unternehmen 2018/2019 von Angriffen betroffen war. In den Jahren 2020/2021 waren es sogar 88 %. Im Jahr 2018/2019 betrugen die wirtschaftlichen Schäden, die durch Diebstahl, Spionage und Sabotage verursacht wurden, 103 Milliarden Euro. Nun hat sich diese Zahl verdoppelt. Die jährlichen Schäden liegen aktuell bei 223 Milliarden Euro.

Abb. 12: Schäden durch Cybercrime bei Unternehmen in Deutschland laut Bitkom.

Haupttreiber des enormen Anstiegs ist laut Bitkom Ransomware. Durch die Erpressungs-Malware werden Dateien auf Computern und anderen Systemen verschlüsselt und unbrauchbar gemacht, anschließend werden die Betreiber erpresst. Die Schäden, die durch Ransomware entstanden sind, haben sich im Vergleich zu den Vorjahren 2018/2019 mehr

als vervierfacht (+358 %). Aktuell sieht jedes zehnte Unternehmen (9 %) seine geschäftliche Existenz durch Cyberattacken bedroht.[12]

Eine Hornetsecurity-Umfrage unter mehr als 820 Unternehmen zeigte zudem, dass **21 % der Befragten bereits Opfer eines Ransomware-Angriffs** wurden.

Trotz des Takedowns von Emotet können Unternehmen also nicht unbedingt aufatmen. Cyberkriminalität bleibt nach wie vor ein lukratives Geschäft, vor allem mit der steigenden Vernetzung.

Fokus auf Microsoft 365

Im April 2020 meldete Microsoft 258 Millionen aktive User der Office 365 Suite. Sollten nur 10 % der genutzten Rechner nicht ausreichend gegen Cyberangriffe geschützt sein, macht das für Hacker ganze 25 Millionen einzelne Ziele, die potenziell leicht zu infiltrieren sind.[13]

Auch der Microsoft Exchange Hack zeigt, dass sogar staatlich gesponserte Hackergruppen Microsoft vermehrt in den Fokus nehmen, da diese wissen, wie viel Druck ein erfolgreicher Angriff auf betroffene Unternehmen und Behörden ausüben kann.

Im Rahmen einer Umfrage zur E-Mail-Sicherheit unter mehr als 420 Unternehmen, die Microsoft 365 für ihre E-Mail-Kommunikation nutzen, konnte Hornetsecurity feststellen, dass **1 von 4 Unternehmen mindestens einmal einer E-Mail-Sicherheitslücke zum Opfer fiel**.

Abb. 13: Hornetsecurity Umfrage unter 420 Unternehmen zum Thema Microsoft 365-Sicherheit

Diese konnten zum größten Teil auf Phishing-E-Mails zurückgeführt werden, die in das Postfach der Nutzer gelangten.

Da sich Microsoft 365 als eine der meistgenutzten Cloud-Anwendungen im Business-Bereich weiterverbreiten wird, ist davon auszugehen, dass auch Hackerangriffe auf die Benutzer weiter ansteigen werden.

Über die Hornetsecurity Group

Hornetsecurity ist ein führender E-Mail-Cloud-Security- und Backup-Provider, der Unternehmen und Organisationen jeglicher Größe weltweit absichert. Das preisgekrönte Produktportfolio deckt alle wichtigen Bereiche der E-Mail-Sicherheit ab: darunter Spam- und Virenfilter, Schutz vor Phishing und Ransomware, sowie rechtssichere Archivierung und Verschlüsselung. Hinzu kommen Backup, Replikation und Wiederherstellung von E-Mails, Endpoints und virtuellen Maschinen. Das Flaggschiffprodukt ist die marktweit umfangreichste Cloud-Sicherheitslösung für Microsoft 365. Mit über 350 Mitarbeitern an 10 Standorten verfügt das Unternehmen mit Hauptsitz in Hannover über ein internationales Netzwerk von mehr als 5.000 Channel-Partnern und MSPs sowie über 11 redundante, gesicherte Rechenzentren. Die Premium-Services nutzen mehr als 50.000 Kunden, darunter Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA und CLAAS.

Quellen

(1) https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, S.6

(2) http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf, S.89 Global Risk Report 2021

(3) https://de.statista.com/statistik/daten/studie/1038510/umfrage/ausgaben-fuer-it-sicherheit-weltweit/

(4) https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/

(5) https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/

(6) https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/

(7) https://www.hornetsecurity.com/de/threat-research/emotet-botnet-takedown/

(8) https://www.hornetsecurity.com/de/threat-research/email-threat-review-juni-2021/

(9) https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/ (Mai, 2021)

(10) https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

(11) Bundeslagebild Cybercrime 2020, BKA, S. 38

(12) https://www.all-about-security.de/management/angriffsziel-deutsche-wirtschaft-mehr-als-220-milliarden-euro-schaden-pro-jahr/

(13) https://securityboulevard.com/2021/06/microsoft-office-365-a-major-supply-chain-attack-vector/

HORNETSECURITY