So wird Windows angegriffen

Neue Techniken und Tools von Cybercrime und staatlichen Hackern

Bild: Andreas Martini

Angriffe auf PC-Systeme sind eine ernstzunehmende Bedrohung. Gut organisierte Banden von Cyber-Erpressern erbeuten Jahr für Jahr Milliarden. Vor allem Windows-Rechner stehen in der Schusslinie – nicht zuletzt, weil sie für Einbrecher häufig offen wie ein Scheunentor sind.

Von Jürgen Schmidt

Windows ist für Kriminelle das beliebteste Angriffsziel unter den Betriebssystemen. Das liegt vor allem an zwei Dingen: Zum einen ist es nach wie vor das am weitesten verbreitete Desktop-Betriebssystem – mit funktionierenden Angriffen auf Windows erschließt sich dem Angreifer ein riesiges Reservoir an Datenschätzen. Zum anderen macht es Windows Angreifern nach wie vor sträflich einfach, ihre Ziele zu erreichen. Diesen Vorwurf werden wir noch genauer beleuchten, wenn wir die konkret eingesetzten Techniken vorstellen.

Doch zunächst zu den Angreifern und deren Zielen: Das sind in der überwältigenden Mehrzahl aller IT-Sicherheitsvorfälle organisierte Kriminelle, also eine Art Cyber-Mafia, die durch Betrug und Erpressung jährlich Milliardenschäden verursacht. Insbesondere die Erpressung hat sich als Goldesel der Cyber-Kriminalität erwiesen. Mit überschaubarem Aufwand erbeuten die Kriminellen dabei echtes Geld in rauen Mengen – und das selbst ohne großes Know-how und mit einem vernachlässigbaren Risiko.

In der Folge hat sich in den letzten Jahren rund um Ransomware – der Begriff bezeichnet zur Erpressung genutzte Schadsoftware und stammt vom englischen „ransom“ für „Lösegeld“ – ein ganzes Cybercrime-Ökosystem mit Dienstleistungen aller Art gebildet. Anbieter von „Ransomware as a Service“ (RaaS) liefern auch unerfahrenen Möchtegern-Kriminellen Komplettpakete aus Tutorials mit Anleitungen, einfach zu bedienenden Software-Baukästen und Infrastruktur für Verhandlungen und Geldübergabe.

Die Opfer dieses Treibens sind vornehmlich Firmen, Organisationen und Behörden, deren Abhängigkeit von funktionierender IT ihre Achillesferse wurde. Aber auch Privatanwender befinden sich nach wie vor im Visier der Kriminellen: Zum einen ist in Zeiten von Homeoffice fast jeder Privat-PC ein potenzielles Einstiegstor in die IT des Arbeitgebers seines Besitzers. So lassen sich die auf einem privaten PC gestohlenen Zugangsdaten gut im Untergrund verhökern. Zum anderen sind auch Privatanwender oft bereit, beispielsweise für den Zugang zu ihrem verschlüsselten Bilderarchiv mit den Fotos von Geburt, Einschulung und Hochzeit der Kinder erkleckliche Summen zu zahlen – „Kleinvieh macht auch Mist“ gilt auch bei Cybercrime.

Typische Vorgehensweise

Die typische Vorgehensweise bei Einbrüchen in Computer lässt sich in drei Phasen unterteilen:

- den eigentlichen Einbruch (Initial Access),
- das Ausbreiten im Netz (Lateral Movement),
- die Erpressung (Impact)

In diesen Phasen kommen nicht nur unterschiedliche Tricks und Werkzeuge zum Einsatz, es ist auch durchaus üblich, dass dahinter verschiedene Akteure stecken. So gibt es einen eigenen Markt, auf dem sogenannte Initial Access Broker (IAB) Zugänge zu Systemen verkaufen. Die auf den Einbruch spezialisierten Kriminellen ernten die infizierten Computer ihrer Opfer systematisch ab und stehlen dort insbesondere alle Zugangsdaten, derer sie habhaft werden können.

Außerdem installieren sie noch ein Hintertür-Programm – einen Remote-Access-Trojaner (RAT), der ihnen zukünftig die volle Kontrolle über das System beschert. Diese Aufgabe übernimmt oft ein sogenanntes Cobalt Strike Beacon: Cobalt Strike ist eine kommerzielle Software, die von Sicherheitstestern bei simulierten Angriffen eingesetzt wird. Aber auch echte Angreifer nutzen sie überaus gern. Eine Webseite, die Cobalt-Strike-Angriffe und mögliche Abwehrmaßnahmen beschreibt, haben wir unter ct.de/y3td verlinkt.

Die gestohlenen Passwörter und den Zugang zum RAT verkaufen die Angreifer in speziellen Untergrundforen und -börsen. Es gibt übrigens Dienstleister, die Privatpersonen und Firmen anbieten, diese IAB-Marktplätze zu überwachen und sie zu benachrichtigen, wenn ihre Daten dort auftauchen sollten. Doch das ist in der Regel das Geld nicht wert. Denn die etablierten IAB-Spezialisten haben Geschäftsbeziehungen zu RaaS-Anbietern, denen sie vorab Zugriff auf ihre Ware anbieten. So landen viele der erbeuteten Daten nie in den für solche Dienstleister einsehbaren Foren.

Einfallstor Office-Dokumente

Zu den wichtigsten Einfallstoren für den „Initial Access“ gehören nach wie vor präparierte Office-Dateien, die bösartige Makros enthalten. Klickt der Anwender beim Öffnen des Dokuments die gelben Balken weg („Inhalt aktivieren“, „Bearbeiten erlauben“), laufen im Hintergrund Befehlssequenzen ab, die etwa eine Datei aus dem Internet nachladen und starten. Das kann dann bereits der oben erwähnte Remote-Access-Trojaner sein, der den Angreifern jederzeit Zugang zum System gibt.

Auf keinem anderen System ist es so einfach, sich mit Schadsoftware aus einer E-Mail zu infizieren, wie bei Windows. Linux, macOS und die Smartphone-Betriebssysteme haben auch ihre Sicherheitsprobleme, über E-Mail angelieferte Malware gehört aber nicht dazu. Unter Windows genügen in der Voreinstellung oft ein, zwei unvorsichtige Klicks, damit die Malware aktiv wird, und das Unheil nimmt seinen Lauf. Und mit täuschend echt gestalteten E-Mails und einer überzeugenden Geschichte gelingt es immer wieder, vor allem unerfahrene Anwender davon zu überzeugen, die notwendigen Klicks tatsächlich durchzuführen.

Doch Microsoft steuert endlich aktiv gegen. Immer mehr Office-Installationen blockieren Makros in Dokumenten, die aus dem Internet stammen, sodass sie unbefangene Nutzer nicht mehr ausführen kön-


Sollten Ihre daten nicht mehr aktuell sein, ändern Sie diese ebenfalls.

1 Anlage

Dat 553912 ~.doc

----Original Message-----

Sehr geehrter Herr [redacted]

anbei erhalten Sie unterzeichnete Preisvereinbarung für 2019.

Freundliche Grüße

[redacted]

Verlag Heinz Heise GmbH & Co. KG
Karl-Wiechert-Allee 10
30625 Hannover

Emotet bei Heise: Mit dieser Mail schaffte es die Emotet-Bande, einen Heise-Mitarbeiter auszutricksen. Die Nachricht zitierte seine eigene E-Mail und sah damit für ihn wie eine ganz normale Geschäfts-Mail aus.

nen. Doch das dafür eingesetzte Mark of the Web ist längst nicht so zuverlässig, wie man sich das wünschen würde. Mehr dazu erklärt ein Artikel auf heise Security [1].

Das LNK-Revival

Als Alternative zu Makros experimentieren die IABs mit verschiedenen Tricks. Das führt zu einem Revival der LNK-Dateien: Das sind Verweise auf andere Programme, die beim Öffnen auszuführen sind; Windows verwendet sie zum Beispiel für Desktopsymbole und Startmenüeinträge. Eine einzelne LNK-Datei ist jedoch verdächtig und jedes bessere Mail-Gateway wird sie als potenzielles Schadprogramm blockieren. Stattdessen bekommt ein Anwender deshalb zum Beispiel ein ISO-Image via Mail – optional noch verpackt in ein Zip-Archiv. Diese Image-Datei bindet Windows beim Öffnen netterweise als Laufwerk ein und zeigt ein Fenster mit etwas wie „Umsatz_Report_2022“ an; die verräterische Endung „.lnk“ versteckt der Explorer selbst dann, wenn Sie Windows anweisen, Erweiterungen bei bekannten Dateitypen anzuzeigen.

Beim Klick auf den angeblichen Report passieren je nach Inhalt der LNK-Datei verschiedene Dinge. In einem typischen Szenario startet Windows via rundll32.exe eine Bibliothek, die sich in einem versteckten Ordner des ISO-Image-Laufwerks befindet und den Schadcode der Kriminellen ausführt, also etwa ein Cobalt Strike Beacon nachlädt und installiert. Ein anderes Angriffsszenario lässt Windows den mächtigen Skript-Interpreter powershell.exe starten, der seine Anweisungen aus der Kommandozeile entnimmt. Das Resultat ähnelt letztlich Szenario 1 – der Rechner ist infiziert.

Updates, Updates, Updates!

Vor allem für Firmen sind extern erreichbare Dienste eine große Gefahr. An vorderster Front stehen VPN-Gateways oder fahrlässigerweise aus dem Internet erreichbare RDP-Zugänge. Oft finden Angreifer auch bei Suchmaschinen oder durch Scans ganzer IP- und Port-Bereiche längst vergessene FTP-Server oder ein nur mal testweise eingerichtetes Content Management System, das nicht mit allen Sicherheitsupdates versehen wurde.

Dabei kommt erschwerend hinzu, dass die Lücken nicht nur in den Programmen stecken, die man eigentlich installiert hat. Software besteht heutzutage aus unzähligen fertigen Komponenten, die die Entwickler in ihre Projekte einbinden. Taucht in einer davon eine Lücke auf, sind all ihre Downstream-Apps anfällig. So traf eine Sicherheitslücke in der Java-Bibliothek Log4j Tausende Applikationen, die damit ihre Protokollierung in Log-Dateien erledigten [2].

Nur in seltenen Fällen kommen bei diesen Angriffen unbekannte Sicherheitslücken, sogenannte Zero Days, zum Einsatz. Die große Mehrzahl der Einbrüche erfolgt über bekannte Schwachstellen, gegen die es bereits Updates gäbe. Ein zu spät eingespieltes Sicherheitsupdate bedeutet fast zwangsläufig, dass man ungebetenen Besuch bekommt.

Passwörter als Problem

Ein weiterer wichtiger Einfallsvektor sind kompromittierte Zugangsdaten. Die erlangen Kriminelle häufig über Phishing. Weil wir dem Thema erst kürzlich einen ausführlichen Schwerpunkt gewidmet haben [3, 4], gehen wir hier nicht weiter darauf ein.

Gern jubeln IABs ihren Opfern sogenannte Infostealer unter. Haben Sie sich schon mal gewundert, wer sich die Mühe macht, gecrackte Versionen von teuren Softwarepaketen zu erstellen und kostenlos im Internet zu verteilen? Oder einen tollen Aim-Bot für den aktuell gehypten First Person Shooter? Das sind nicht selten Initial Access Broker, die mit dem gecrackten Photoshop auch gleich einen maßgeschneiderten Infostealer verteilen. Der sammelt alle auf dem System gespeicherten Passwörter ein, die der IAB danach zu Geld machen kann.

Da schlägt eine weitere Windows-Schwäche zu: Anders als moderne Smartphone-Betriebssysteme schottet Windows die verschiedenen Applikationen, die ein Anwender auf dem System ausführt, so gut wie gar nicht gegeneinander ab. So kann das gecrackte Photoshop auf alle Firefox-Dateien zugreifen. Das funktioniert wohlgemerkt ganz ohne Admin-Rechte, einfach mit Code im Kontext des angemeldeten Benutzers. Auf einem iPhone oder Android-Smartphone wäre das hingegen so nicht möglich. Dort sind alle Apps gegeneinander abgeschottet. Vereinfacht kann man sich das so vorstellen, dass jede App unter Android einen eigenen Benutzerkontext bekommt und damit die Photoshop-App keinen Zugriff auf Dateien oder gar den Arbeitsspeicher der Firefox-App hat.

Ganz einfach macht es dem Angreifer etwa Microsoft Teams. Dort liegt ein Token im Benutzerverzeichnis, das ein Infostealer nur einsammeln und an seinen Herrn und Meister schicken muss, um diesem den Zugang zum Teams-Account des Opfers zu geben (Details via ct.de/y3td). Im Idealfall verschlüsseln Anwendungen solche Daten deshalb etwa mit dem Data Protection API (DPAPI) von Windows. Damit genügt es nicht mehr, dass der Angreifer die Dateien seines Opfers lesen kann.

Eine große Hürde ist das für einen Infostealer allerdings nicht, jedenfalls wenn er seinen Code bereits im Kontext des jeweiligen Benutzers ausführt: Die DPAPI-Funktion `CryptUnprotectData()` verwendet die Zugangsdaten des aktuell angemeldeten Benutzerkontos als Schlüssel. Immerhin schützt die Verschlüsselung aber Benutzerdaten vor Schnüffelsoftware, die in einem anderen Kontext läuft,

etwa unter dem zu einem lokalen Webserver gehörenden Konto.

Die Sicherheitsfirma Palo Alto dokumentiert in einem Blog-Beitrag (Link siehe ct.de/y3td) exemplarisch, wie Angreifer gespeicherte Benutzerdaten in Chrome, Firefox, WinSCP, OpenVPN und Git auslesen. Frei verfügbare Tools wie WebBrowserPassView und DataProtectionDecryptor von Nirsoft können das auch. Verhindern ließe sich das, wenn Windows vor dem Entschlüsseln der Passwörter via DPAPI jedes Mal eine Authentifizierung des Anwenders anfordern würde, sei es per Hello-Kamera oder per Fingerabdruck-Scan – macht es aber nicht.

Sie sind drin

Insbesondere die sogenannten Affiliates von RaaS-Banden – Click-&-Shoot-Kriminelle ohne eigenes Infektions-Know-how – kaufen Zugangsdaten gerne bei IABs ein. Sie probieren sie systematisch durch, auch bei anderen Diensten. Das nennt sich Credential Stuffing: Irgendwann passt etwa ein im privaten Browser gespeichertes Passwort für den Firmen-Mail-Zugang wegen des Single-Sign-on-Konzepts auch beim VPN-Zugang ins Firmennetz und sie sind drin. Oder die Affiliates geben etwas mehr Geld aus und kaufen betriebsbereite RAT-Zugänge, um sich auf dem infizierten PC umzusehen. Diese Aktivitäten können durchaus auch ein bis zwei Wochen nach der ursprünglichen Infektion anlaufen, weil die Zugangsdaten zunächst durch mehrere Hände gingen oder sich bei den Banden stauen.

Das weitere Vorgehen unterscheidet sich dann bisweilen nach den vorgefundenen Einstellungen und Programmen. Die Bumblebee-Malware lädt auf Systemen, die Mitglied in einer Arbeitsgruppe wie WORKGROUP sind, einen Infostealer, der den vermuteten Privat-PC nach Passwörtern und Ähnlichem durchsucht. Ist das Opfer hingegen Mitglied in einer Windows-Domäne, wie das typischerweise in Firmen der Fall ist, landet dort sofort ein Cobalt Strike Beacon, über dessen Hintertürfunktion sich recht bald ein Einbrecher persönlich ein genaueres Bild verschafft.

Schadsoftware wird häufig ganz klassisch über Dateien nachgeladen und ausgeführt. Doch es kommen vermehrt auch ausgefeiltere Techniken zum Einsatz. Da holt sich ein Loader den verschlüsselten Schadcode aus dem Internet und dechiffriert ihn im eigenen Arbeitsspeicher. Dann besorgt er sich ein Handle für den Zugriff auf einen laufenden, legitimen Prozess wie den Explorer und reserviert dort Arbeitsspeicher. In den kopiert der Loader den Schadcode und startet ihn als eigenen Thread.

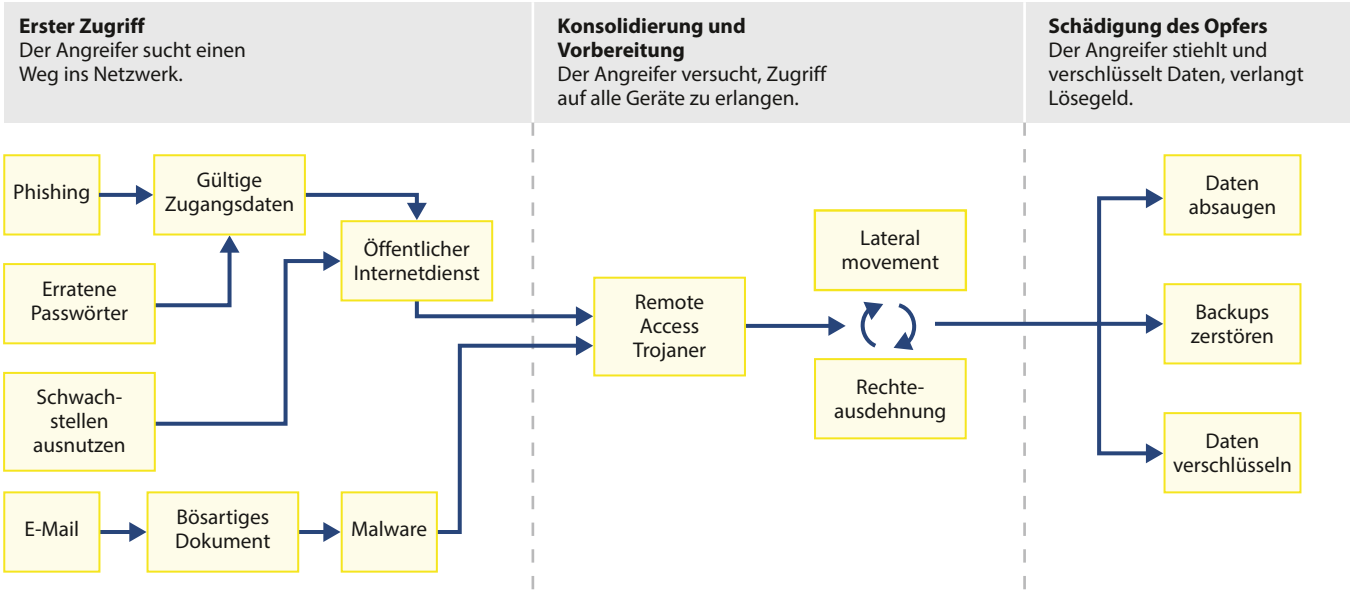
Das hat mehrere Vorteile: Zum einen sieht es so aus, als ob die Zugriffe auf Dateien und Netzwerk vom Windows-eigenen Explorer stammen, was Sicherheitssoftware beruhigen soll. Zum anderen landet der Schadcode nie auf der Festplatte des Systems. Das reduziert die Gefahr einer Entdeckung durch Wächter wie Antivirensoftware, die gezielt alle Dateien auf Anzeichen von Schadsoftware durchsucht. Außerdem minimiert es die Gefahr, dass der wertvolle Code etwa im Rahmen einer forensischen Analyse in die Hände von Sicherheitsfirmen fällt.

Andererseits birgt diese Methode neue Möglichkeiten, verdächtiges Verhalten zu bemerken. So überwachen Extended Detection & Response Systeme (EDR) die Systemaufrufe aller Prozesse. Bei typischen Malware-Aktivitäten wie dem Zugriff via `WriteProcessMemory()` und `CreateRemoteThread()` auf den Explorer-Prozess terminiert das EDR den Prozess und löst einen Alarm aus. Die Angreifer reagieren darauf, indem sie die EDR-Überwachungs-Hooks deaktivieren oder umgehen. Das Hase/Igel-Rennen ist in vollem Gang.

Eine andere Technik, die verräterische Dateien vermeidet und Windows-eigene Softwaresperren wie Software Res-

Ablauf eines Ransomware-Angriffs

Einbrüche in Computer laufen typischerweise in drei Phasen ab: Nachdem sich die Angreifer Zugang zu einem ersten System verschafft haben, versuchen sie, ihren Einfluss möglichst unbemerkt auf andere Rechner im Netzwerk auszuweiten. Erst dann verschlüsseln sie Daten oder kopieren sie auf eigene Server, um anschließend ihr Opfer zu erpressen.



triction Policies (SRP) und App Locker umgeht, nennt sich Living Off The Land (LOL) – sinngemäß „mit dem arbeiten, was man vorfindet“. Dabei nutzen die Angreifer ganz normale Windows-Bordmittel – die LOLBins – für ihre Zwecke, also etwa den Download eines Hintertür-Programms via certutil.exe auf der Kommandozeile. Mit LOLBins unterlaufen Angreifer EDR-Systeme, denn es handelt es sich ja um legitime Programme. Eine aktuelle Aufstellung typsicherer LOLBins und wie sie genutzt werden, gibt es unter lolbas-project.github.io.

Quest for Local Admin

Nach dem Einbruch geht es den Einbrechern zunächst darum, den Zugang zum System auszuweiten und sich im Netz zu anderen Systemen weiterzuhangeln (Lateral Movement). Dazu versuchen sie, sich die Rechte eines lokalen Administrators zu verschaffen. Wenn der Anwender, dessen Account gekapert wurde, Mitglied der Gruppe der Administratoren ist und dieser lediglich durch die Benutzerkontensteuerung (User Account Control, UAC) beschränkt wird, haben die Eindringlinge leichtes Spiel. Es gibt reihenweise Demos, wie sich die UAC austricksen lässt, um uneingeschränkte Adminrechte zu ergattern (siehe ct.de/y3td). Etwas schwerer macht man es den Kriminellen, indem man den Regler der Benutzerkontensteuerung (in den Einstellungen nach „UAC“ suchen) ganz nach oben schiebt. Trotzdem sieht auch Microsoft die UAC nicht als zu verteidigende Security-Grenze an. Und Microsoft wird auch erklärtermaßen keine Security-Updates liefern, die UAC-Exploits verhindern könnten.

In Firmennetzen mit administrierten PCs gehören normale Benutzerkonten eher selten zur Gruppe der Administratoren. Deshalb nutzen die Angreifer dort sogenannte Privilege-Escalation-Lücken. Penibel gepflegte Sicherheitsupdates würden solche Rechteerweiterungen oftmals verhindern, doch dem Angreifer genügt ein einziger, nicht rechtzeitig installierter Patch. Nicht aussterben will auch grottige Software, die noch mit Admin-Rechten läuft, aber bei den Zugriffsrechten auf Dateien und Verzeichnisse schlampt und sich so zum Beispiel eine Malware-DLL unterjubeln lässt. Hat ein Angreifer erst einmal einen Fuß in der Tür, gelingt es ihm erschreckend häufig auch, sich Adminrechte zu verschaffen. Eine erschütternd lange Liste an Tools und Methoden dazu pflegt beispielsweise das GitHub-Projekt „PayloadsAllTheThings“ (siehe ct.de/y3td).

Quest for Domain Admin

Mit den Rechten des lokalen Administrators wird der Rechner erneut auf Zugangsdaten geflöht. Eine zentrale Anlaufstelle dafür ist der Local Security Authority Server Service, kurz LSASS, der alle Anmeldevorgänge durchführt. Dazu hält der LSASS-Prozess die gehashte Version des Passworts im Arbeitsspeicher vor. Dessen Inhalt kann man etwa mit dem – legitimen und von Microsoft bereitgestellten – Werkzeug ProcDump aus der Sysinternals Suite in eine Datei schreiben:

```
procdump64 -ma lsass.exe lsass.dmp
```

Spezielle Tools wie Mimikatz extrahieren aus dieser Datei dann unter anderem die NTLM-Hashes angemeldeter Benutzer. Damit kann sich der Angreifer dann ebenfalls bei allen Diensten im Netz anmelden und sich beispielsweise via RDP von System zu System hangeln. Ist auf einem dieser Systeme ein Domänen-Administrator angemeldet, findet der Angreifer auch dessen NTLM-Hash im Arbeitsspeicher des LSASS-Prozesses. Damit schwingt er sich zum König des Windows-Netzes auf.

Um das zu verhindern, hat Microsoft eigentlich den Credential Guard eingeführt, der den LSASS in eine besonders geschützte virtuelle Umgebung verschiebt, auf die selbst der Administrator oder ein Account mit Systemrechten nicht zugreifen kann. Der Haken dabei ist, dass Credential Guard den teuren Enterprise-Versionen von Windows vorbehalten ist; Heimanwender und auch kleinere Firmen mit Windows-Home- oder -Pro-Lizenzen schauen in die Röhre. Überhaupt setzt sich bei Microsoft immer stärker die Philosophie „Windows ist billig, Security kostet extra“ durch und führt dazu, dass man Sicherheitsfunktionen als Lockmittel für teurere Lizenzen verwendet oder sie sich für viel Geld extra bezahlen lässt [5].

Impact

Mit den erbeuteten Zugängen gehen die Angreifer dann auf Raubzug und exfiltrieren alles an Daten, was ihnen wertvoll erscheint: Dokumente, Datenbank-Dumps und Quellcode landen dabei auf externen Servern. Typischerweise nutzen die Angreifer dazu öffentlich verfügbare Tools wie Rclone, um ganze Verzeichnisbäume in einen speziell dafür angemieteten Cloud-Speicher bei Hostern wie Mega zu kopieren.

Erst wenn sie das Gefühl haben, alles Erreichbare abgeerntet zu haben, kommt die Verschlüsselungssoftware zum Einsatz. Damit die auf möglichst vielen Rechnern im Netz gleichzeitig zuschlägt, nutzen die Cybercrime-Banden gerne Tools wie psexec, ebenfalls von Sysinternals. So bindet die Ransomware Netwalker mit folgendem Kommando auf allen Systemen der Domain eine Dateifreigabe als Laufwerk Q: ein und startet von dieser aus ein PowerShell-Skript, das letztlich alle wichtigen Daten auf dem Rechner verschlüsselt:

```
C:\psexec.exe @ip-list.txt -d cmd /c ↵
↳"net use q: ↵
↳\\DomainController\DomainName /user:↵
↳DomainName\administrator Passwrt &; ↵
↳powershell -EP ByPass -NoLogo ↵
↳-NoProfile -windowstyle hidden ↵
↳-NoExit -File q:\P100119.ps1"
```

Dieses Kommando nutzt keine Sicherheitslücken mehr aus, sondern arbeitet völlig regulär mit den Credentials des Domänen-Administrators. Das gestartete PowerShell-Skript startet die eigentliche

Wer nicht zahlt, wird bloßgestellt: Die Erpresserbande „Cuba Ransomware“ präsentiert erbeutete Datensätze auf einer Webseite im Tor-Netz.

Ransomware – ebenfalls von Q: – und hinterlegt anschließend die Lösegeldforderung als neuen Desktop-Hintergrund. In aktuellen Erpressungsversuchen sollen die Opfer häufig gleich zweimal zahlen: erstens für den Schlüssel, mit dem sie ihre Daten wiederherstellen können, und zweitens für die Versicherung der Kriminellen, dass man die kopierten Daten lösche und nicht an Dritte weitergebe.

APT, Hacktivists & Trolle

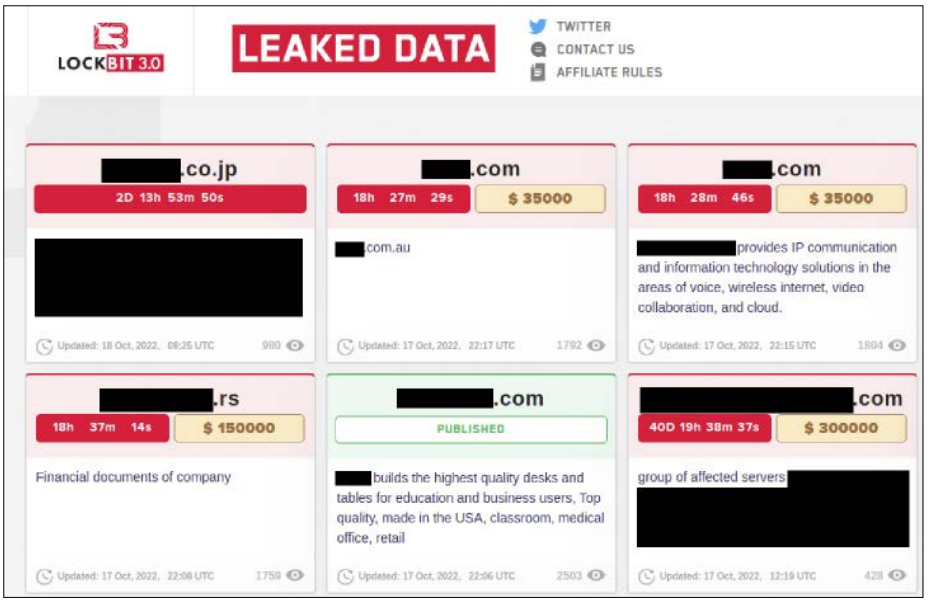
Neben dem organisierten Verbrechen, dem es vor allem um Geld geht, gibt es auch staatliche gesteuerte Angreifergruppen. Die agieren prinzipiell ähnlich, können jedoch auf viel umfangreichere Ressourcen zugreifen und damit auch technisch anspruchsvollere Angriffstechniken einsetzen. Der größte Unterschied ist jedoch in der Zielsetzung begründet: Sowohl für Spionage als auch für gezielte Sabotage am Tag X ist es erforderlich, möglichst unauffällig vorzugehen.

Deshalb agieren diese sogenannten Advanced Persistent Threats (APT) nicht in die Breite, sondern extrem zielgerichtet und vorsichtig, um keine Alarme auszulösen. Es ist nicht unüblich, dass APT-Gruppen über Monate oder sogar Jahre hinweg unentdeckt im Netz ihrer Opfer agieren. Privatanwender und kleinere Unternehmen haben von APTs in der Regel nur wenig zu befürchten. Außer natürlich, sie haben sich etwa politisch besonders exponiert oder können als Sprungbrett zu den eigentlich anvisierten, großen Fischen dienen.

Ferner gibt es auch noch weniger gut organisierte Angreifer, die häufig aus politischen Gründen aktiv werden. Dazu gehören Aktivisten wie die ukrainische IT-Army oder vergleichbare russische Gruppen, die vor allem Dienste mit DDoS-Attacken lahmlegen oder leicht zugängliche Daten stehlen und veröffentlichen.

So schützen Sie sich

Ähnlich, wie die Angriffe mehrstufig erfolgen, sollte auch das Schutzkonzept nicht alles auf eine Karte setzen, sondern in Schichten angelegt sein. Sicherheitsexperten nennen das „Defense in Depth“. Die Grundidee ist, dass auch nach einer Infektion mit Schadsoftware noch nicht automatisch alles verloren ist, sondern man realistische Chancen hat, den Einbrecher zu bemerken und rechtzeitig wieder rauszuwerfen, bevor er ernsten Schaden anrichten kann.



Lockbit ist einer der großen Anbieter von „Ransomware as a Service“ und arbeitet mit Doppel-Erpressung. Wer nicht rechtzeitig zahlt (grün), dessen Daten werden auf einer eigenen Leak-Site veröffentlicht.

Der erste Verteidigungswall versucht, es dem Angreifer so schwer wie möglich zu machen, überhaupt einen Fuß in die Tür zu bekommen. Dazu gehören technische Maßnahmen, darunter Sicherheitsupdates zügig einzuspielen und konsequent Zweifaktor-Authentifizierung zu nutzen, aber auch verantwortungsbewusst mit E-Mails umzugehen. Welche Windows-Einstellungen es Eindringlingen so schwer wie möglich machen, lesen Sie im folgenden Artikel. Und ab Seite 28 nehmen wir „Smart App Control“ unter die Lupe, eine neue Sicherheitskomponente, die Microsoft gerade erst in Windows 11 eingeführt hat.

Die nächste Verteidigungsschicht soll den Angreifer daran hindern, sich festzusetzen und weiter auszubreiten. Dazu gehören Härtungsmaßnahmen aller Art, also unter anderem die Nutzung von Software Restriction Policies und andere White-Listing-Lösungen. Ab Seite 32 erfahren Sie mehr dazu.

Ein wichtiger Baustein ist auch das sogenannte Monitoring und Alerting, bei dem es darum geht, Angreifer in flagranti zu ertappen. Das muss kein teures Intrusion Detection System sein. Stellen Sie Fallen und Stolperdrähte auf, die ein Angreifer mit seinem Treiben auslöst. Legen Sie dazu zum Beispiel einen ungenutzten Windows-Account auf dem System an, dessen Passwort Sie in Ihrem Arbeitsverzeichnis an passender Stelle speichern. Dann richten Sie alles so ein, dass jeder Login einen Alarm auslöst, und Sie haben Ihren ersten Honeypot gebastelt.

Und schließlich muss man für den Ernstfall vorsorgen. Das beginnt mit guten Backups – kein Backup, kein Mitleid! – und geht bis zu vollständig ausgearbeiteten Notfallplänen. Insbesondere Firmen sollten sich vorab ganz konkret Gedanken machen, wie sie auf – die ganz sicher eintretenden! – Sicherheitsvorfälle reagieren, und das auch dokumentieren. Und zwar tunlichst nicht im Netz, das dann vielleicht schon der Angreifer kontrolliert, sondern ganz klassisch ausgedruckt auf Papier.

(hos@ct.de) c't

Jürgen Schmidt ist Senior Fellow Security bei Heise und baut mit heise Security Pro eine Community für IT-Professionals auf, in der aktuelle Angriffe, Probleme der täglichen Praxis sowie aktuelle und künftige Technik diskutiert werden: www.heise.de/heisec-pro.

Literatur

[1] Jürgen Schmidt, MS-Office: So funktioniert der neue Office-Makroschutz: heise.de/-7164134
[2] Mirko Dölle, Kleine Ursache, Super-GAU, Sicherheitslücke Log4Shell: Internet in Flammen, c't 2/2022, S. 10
[3] Ronald Eikenberg, Gute Mails, böse Mails, Gefahrloser Umgang mit E-Mails, c't 19/2022, S. 16
[4] Ronald Eikenberg, E-Mails durchleuchtet, Phishing-Mails erkennen und abwehren, c't 19/2022, S. 18
[5] Oliver Klarmann, Microsoft und Emotet: Makroschutz in Office 365 nur für Konzerne: heise.de/-4664218

Weitere Informationen, Tools zum Download: ***ct.de/y3td***