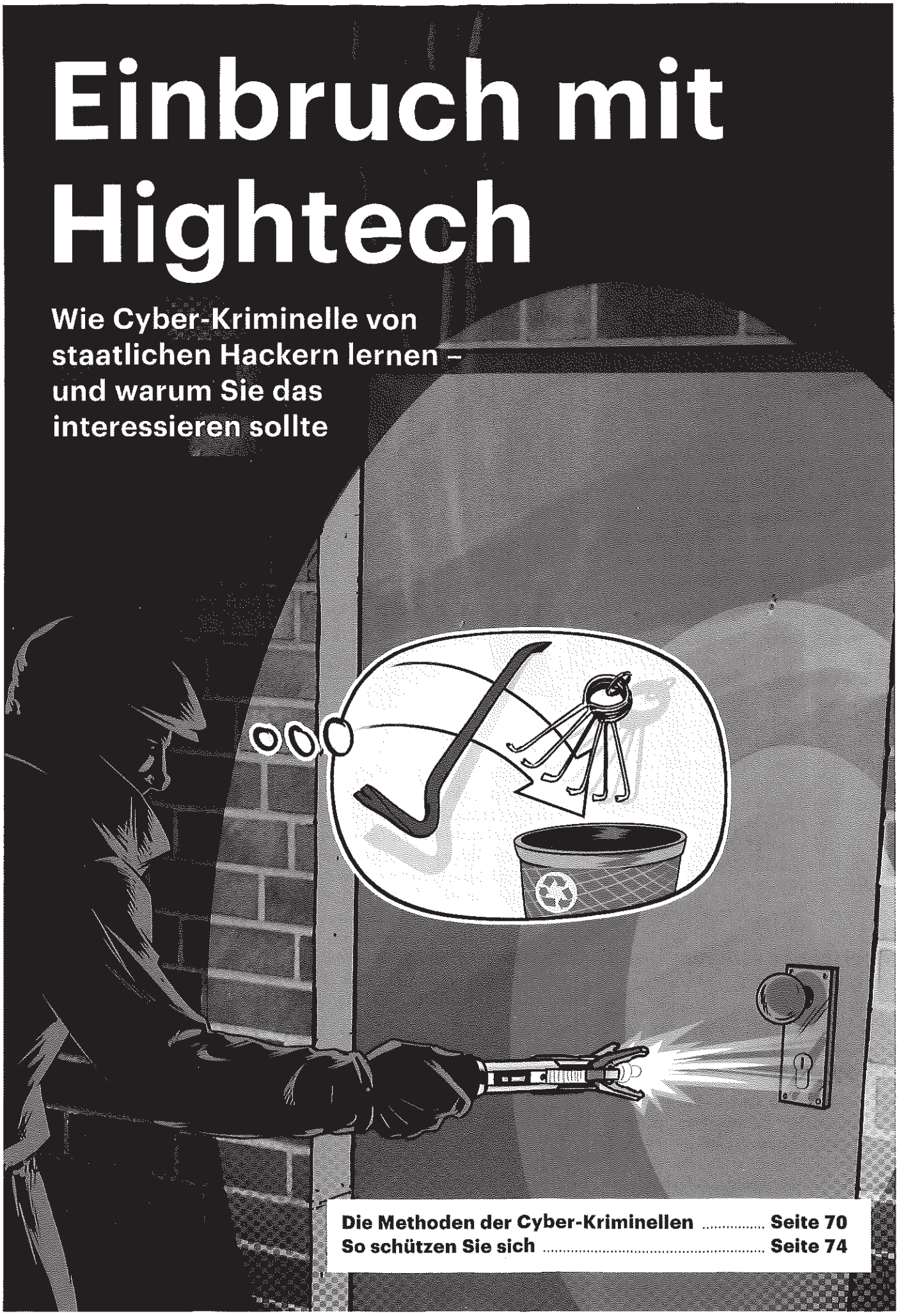
Einbruch mit Hightech

Wie Cyber-Kriminelle von staatlichen Hackern lernen – und warum Sie das interessieren sollte



Man muss nicht mehr bei wichtigen Regierungsbehörden oder einem Rüstungskonzern arbeiten, um Angriffen auf höchstem technischen Niveau ausgesetzt zu sein. Cybercrime-Banden wie Emotet machen sich die Methoden staatlicher Profi-Hacker zu eigen und greifen damit höchst erfolgreich ganz normale Firmen an. Bereits morgen kann das auch Sie treffen.

Von Jürgen Schmidt

Die von Regierungen in Auftrag gegebenen Hacking-Aktivitäten zielen meist auf Spionage oder Sabotage. Für die Betreiber kritischer Infrastruktur und internationale Großkonzerne ist die Bedrohung durch solche Advanced Persistence Threats (APTs) bereits allgegenwärtig und man arbeitet daran, sich dagegen zur Wehr zu setzen.

Doch wer die IT eines mittelständischen Unternehmens am Laufen hält, hat in aller Regel ganz andere Probleme. Schutz vor Spionage und gezielte Sabotage durch Hacker stehen dort weit unten auf der Prioritätenliste. Wenn es um die Sicherheit geht, versucht man bestenfalls Maßnahmen gegen generelle Viren- und Spam-Aktivitäten umzusetzen. Doch die genügen nicht mehr.

Denn Cybercrime-Gangs schauen sich vermehrt die Tricks und Tools der APT-Cracks ab und attackieren damit ganz normale Firmen. Das trifft dann wie im Dezember einen Elektrodienstleister genauso wie eine Stadtverwaltung, eine Arztpraxis oder eine Bäckerei. Die sind auf diese für sie neuartige Bedrohung nicht vorbereitet und weitgehend schutzlos.

Auch bei mittelständischen Firmen, Vereinen und öffentlichen Institutionen geht ohne IT schon lange nichts mehr. Oder anders herum: Wer die IT unter seine Kontrolle bringt, hat den perfekten Hebel, dieses Unternehmen nach allen Regeln der Kunst auszunehmen – also etwa durch Erpressung mal eben fünf- oder sechsstellige Beträge zu ergattern.

Das macht diese Firmen beziehungsweise deren Mitarbeiter zu prädestinierten Opfern für Attacken durch ambitionierte Cybercrime-Gangs, die vom Klein-Klein des Online-Banking-Betrugs genug haben und in die nächsthöhere Liga aufsteigen wollen. Genau das haben die Emotet- und die Dridex-Bande 2018 so erfolgreich umgesetzt, dass man für 2019 mit zahlreichen Nachahmern rechnen muss.

Gezielte Angriffe

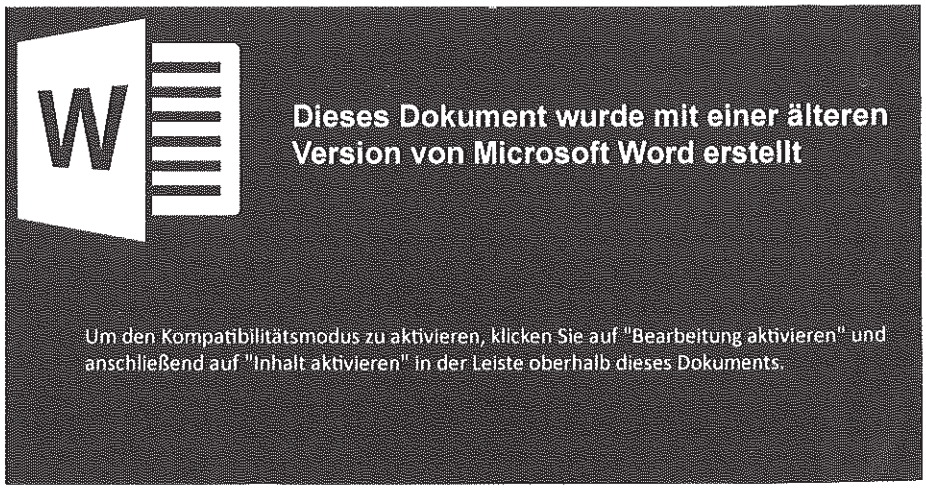
Wenn APT-Hacker in das Netz eines Konzerns eindringen wollen, greifen sie meist zum sogenannten Spear-Phishing. Dabei werden einige wenige Zielpersonen zunächst über Wochen hinweg beobachtet und ausgeforscht. Man sammelt dabei alle möglichen Informationen wie ihre Rolle im Unternehmen, direkte Kontakte, Social-Media-Aktivitäten, darüber dann mögliche Hobbys und so weiter.

Erst dann schlagen die Hacker zu. Zum Beispiel mit einer Mail, die vom direkten Vorgesetzten stammt und sich über einen verpassten Termin beschwert. Ziel ist es, den Empfänger dazu zu verleiten, einen Dateianhang zu öffnen, der seinen Rechner infiziert. Wenn das beim ersten Mal nicht klappt, probiert es der Angreifer wieder – und wieder. Genau dafür steht die Persistenz in APT. Spear-Phishing ist unheimlich effizient. Es ist keine Frage, ob die Hacker ihr Ziel erreichen, sondern nur wann. Irgendwann sind sie drin.

Und vielleicht haben auch Sie in den letzten Monaten einen dieser Rechnungs-Trojaner bekommen, der angeblich von einem Kollegen stammte und sehr gut gemacht war? Keine Angst – Sie sind nicht ins Visier der staatlichen APT-Hacker von Fancy Bear oder Sandworm geraten. Aber es war auch kein Zufall, sondern ein wesentlicher Bestandteil des neuen Geschäftsmodells einer Cybercrime-Gruppe. Die nutzen nämlich eine Art Spear-Phishing auf Massenbasis – Dynamit-Phishing sozusagen.

Die Emotet-Gang trat erstmals 2014 mit Online-Banking-Trojanern in Erscheinung, die vor allem Kunden deutscher Banken im Visier hatten. 2017 brachten sie Trickbot ins Spiel, der einen sehr ausgefeilten Nachlade-Mechanismus aufweist. Über den wurde auf infizierten Systemen Schad-Software anderer Gangs installiert. Natürlich geschah das gegen Geld: „Pay Per Install" lautete das neue Motto. In diesem Kontext kam dann im Gefolge von Emotet-Infektionen sehr häufig auch Ransomware auf die Rechner der Opfer.

2018 hat Emotet weiter dazugelernt. Der Trojaner ist jetzt ein sehr universelles Tool zur Erforschung von Netzwerken und dem Diebstahl von Passwörtern. Besonders bemerkenswert ist das kürzlich eingeführte Abernten von Microsoft Out-



Mit solchen Tricks wollen die Trojaner den Anwender zum Aktivieren der Word-Makros bringen. Wer auf „Inhalt aktivieren" klickt, hat verloren.

Bild: Kryptos Logic

Emotet verbreitet sich weltweit in erschreckendem Ausmaß.

look – auch als Outlook-Harvesting bezeichnet. Dabei fragt der Schädling über das Outlook-API (via mapi.dll) Informationen zu den E-Mails seines Opfers ab – und zwar insbesondere volle Namen und E-Mail-Adressen aller registrierten Sender und Empfänger des letzten halben Jahres.

Daraus baut Emotet eine Art sozialen Graphen, den er an den Command & Controll-Server der Gangster schickt. Die wissen damit, wer mit wem Mails austauscht und wie häufig. Die Emotet-Gang hat damit wertvolle Informationen nicht nur zu den Opfern, die sich mit dem Trojaner infiziert haben, sondern auch zu deren Kontakten. Und die nutzen sie weidlich aus.

Diese Informationen waren die Basis für die massiven Malspam-Wellen Ende 2018, die viele Firmen völlig unvorbereitet trafen. Da kam dann plötzlich eine angebliche Mail von einem Geschäftspartner, dass eine Rechnung noch nicht bezahlt sei. Viel zu häufig öffnete ein verdatterter Sachbearbeiter die angehängte Rechnungskopie und das Unheil nahm seinen Lauf. Eine solche Mail im Postfach heißt übrigens nicht zwangsläufig, dass man selbst oder der angebliche Absender vorher Opfer einer Emotet-Infektion waren. Emotet kann die Verbindung auch aus einer Mail an einen größeren Adressatenkreis extrahiert haben.

Interessant ist, dass das Harvesting nur bei Outlook-Nutzern erfolgt. Das sagt einiges über die anvisierte Zielgruppe aus. Das vor allem im privaten Umfeld eingesetzte Windows Mail bietet zwar durchaus vergleichbare Funktionen, wird aber ignoriert. Privatnutzer sind offenbar für Emotet nicht mehr so interessant.

Gut gefälscht

Auf Outlook zugeschnitten sind auch die Tricks, die den gefälschten Absender glaubhaft erscheinen lassen. Das massenhafte Fälschen der tatsächlichen Mail-Absenderadresse ist wegen der mittlerweile recht flächendeckend umgesetzten Maßnahmen gegen Spam nicht mehr richtig praktikabel. Deshalb baut Emotet die angebliche Absenderadresse in den Anzeigenamen des Absenders ein. Die volle Adresse sieht dann etwa so aus:

```
"Angela Merkel <angie@kanzleramt.de>"↴
                ↳<irgendwo@sonstwo.com>
```

wobei `irgendwo` ein gehacktes Mail-Konto ist, über das die Mail tatsächlich verschickt wurde. Die kann man aber etwa mit zusätzlichen Leerzeichen einfach aus dem Blickfeld schieben. Wer nicht ganz genau hinschaut, sieht in Outlook nur eine scheinbar echte Mail aus dem Kanzleramt – oder bei einem Emotet-Trojaner die eines Kollegen.

Und es zeichnet sich bereits ab, dass die Qualität dieser Malspam-Mails weiter zunehmen wird. Denn seit einigen Monaten besorgt sich Emotet zusätzlich zu den Mail-Adressen auch die Mails selber – genauer gesagt, die ersten 16 KByte mit dem Kopf und dem Text der Nachricht. Dass es dabei keine Rücksicht auf Datei-Anhänge nimmt, deutet darauf hin, dass es nicht um Spionage geht. Vielmehr sieht es sehr nach einem Versuch aus, die künftigen Dynamit-Phishing-Kampagnen noch besser auf ihre Ziele zuzuschneiden. So sollte man 2019 mit Trojaner-Mails rechnen, die sich mit korrekter persönlicher Anrede, Grußformel und passender Mail-Signatur schmücken. Mit Machine Learning und anderen KI-Verfahren ließe sich das auch durchaus automatisieren. Selbst ein direkter Anschluss an einen bereits existierenden Kommunikationsfaden ist denkbar.

Die Umstellung des Geschäftsmodells von Emotet ist aus Sicht der Kriminellen ein voller Erfolg – und für die Opfer ein riesiges Problem. Das US-CERT bezeichnet Emotet in einer kürzlich veröffentlichten Warnung bereits als „eines der teuersten und zerstörerischsten Schadprogramme, die den öffentlichen und privaten Sektor bedrohen". Das deutsche BSI stößt ins gleiche Horn: „Emotet ist nach unserer Einschätzung ein Fall von Cyber-Kriminalität, bei der die Methoden hochprofessioneller APT-Angriffe adaptiert und automatisiert wurden", erklärt BSI-Präsident Arne Schönbohm die neuartige Qualität der Angriffe. Man beobachte dabei Schäden von mehr als einer Million Euro schon bei einzelnen Vorfällen.

Der nächste Schritt

Diese enormen Schäden stammen natürlich nicht von dem einzelnen Rechner, der durch ein unvorsichtiges Öffnen des speziell präparierten Dokuments infiziert wurde. Vielmehr resultieren sie aus der nachgeladenen Malware. Die nutzt dann etwa einen Exploit namens EternalBlue, um sich im Netz der Firma auszubreiten. Dieser Exploit stammt ursprünglich aus dem Arsenal des NSA, die ihn über viele Jahre für genau denselben Zweck einsetzte.

Wie verheerend EternalBlue sein kann, bewiesen bereits WannaCry und NotPetya, die für Milliardenschäden sorgten. Gegen die ausgenutzte Schwachstelle gibt es zwar schon seit 2017 Sicherheits-Updates von Microsoft. Doch die haben offenbar längst nicht alle Firmen flächendeckend eingespielt, sodass EternalBlue immer noch reichlich Opfer findet.

Dass es noch schlimmer kommen kann, wenn man einmal Cyber-Kriminelle im Netz hat, zeigen die Aktivitäten der Dridex-Gang. Auch die war ursprünglich auf Online-Banking-Betrug in großem Maßstab spezialisiert. In den letzten Jahren wurde es recht still um sie. Doch wie ein im Herbst veröffentlichter Bericht der Sicherheitsfirma CrowdStrike dokumen-

tiert, hat sich die Gruppe keineswegs zur Ruhe gesetzt.

Vielmehr hat sie gezielt aufgerüstet, um auf einem anspruchsvolleren Spielfeld zu bestehen: Der Erpressung von Firmen, Behörden und öffentlichen Institutionen. Und sie setzen dabei auf Methoden und Tools, die zwar bereits aus dem APT-Umfeld bekannt, für weniger sicherheitsorientierte Firmen jedoch weitgehend neu sind.

Ausbreitung im Netz

Die Dridex-Gang nutzt dabei – ähnlich wie mittlerweile auch viele APT-Gruppen – öffentlich verfügbare Angriffswerkzeuge. So kommt ein bekannter UAC-Bypass zum Einsatz, der den Windows Event Viewer ausnutzt, um die Einschränkungen der Benutzerkontensteuerung zu umgehen. Er beruht darauf, dass der auf höchster Integritätsstufe laufende Event Manager einen beschreibbaren Registry-Key ausliest, um dort spezifizierte Programme zu starten (`HKCU\Software\Classes\ms-settings\shell\open\command`).

Mit Administrator-Rechten ausgestattet, breiten sich die Hacker systematisch im Netz aus – die mit der Aufklärung von APT-Vorfällen beauftragten Experten haben für diesen Angriffsschritt den Begriff „Lateral Movement" geprägt. Auch hier nutzt die Dridex-Gang ein Werkzeug, das APT-Experten vertraut ist: Mit Mimikatz kratzen sie Authentifizierungs-Tokens wie Passwörter, NTLM-Hashes und Kerberos-Tickets aus dem Arbeitsspeicher infizierter Rechner.

Mit denen hangeln sie sich auf andere Rechner im Netz weiter. Dabei nutzen sie Funktionen des öffentlich verfügbaren Toolkits Powershell Empire unter anderem zum Download und zur Installation permanenter Hintertüren. Das wichtigste Ziel ist es, einen Controller der Windows-Domäne zu kapern. Ist das einmal gelungen, gehört ihnen quasi das Firmennetz. Über den Domain Controller rollen die Kriminellen dann mit Gruppenrichtlinien und Batch-Skripten einen Erpressungs-Trojaner namens BitPaymer auf allen Systemen im Netz aus.

Erst wenn die Cyber-Gangster die Analyse- und Ausbreitungsphase abgeschlossen haben, geben sie den Startschuss zur Aktivierung von BitPaymer. Der verschlüsselt dann auf einen Schlag im ganzen Netz der Firma wichtige Daten. Anschließend präsentieren die Erpresser ihre Lösegeld-Forderung. Dabei orientieren sie sich nicht nur am vermuteten Wert der vorgefundenen Daten sondern auch an dem eines störungsfreien IT-Betriebs. Das sind dann bei kleineren Firmen niedrige fünfstellige Beträge. Aber die Sicherheitsfirma CrowdStrike berichtet auch von Vorfällen, etwa in Krankenhäusern, in denen mehrere hunderttausend US-Dollar in Bitcoins gefordert und bezahlt wurden.

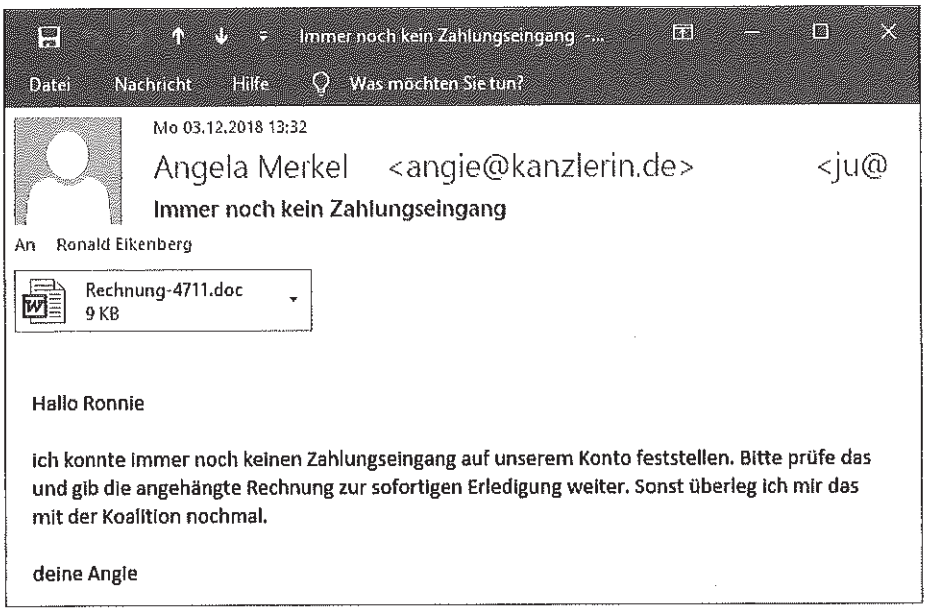
Man mag sich gar nicht ausmalen, was passiert, wenn die Kriminellen hinter Emotet und Dridex zusammenarbeiten: Dynamit-Phishing kombiniert mit anschließender Komplettübernahme der IT-Infrastruktur. Das Problem ist, dass viele Firmen und auch öffentliche Einrichtungen auf Angriffe wie die der Emotet- und Dridex-Gang so gut wie nicht vorbereitet sind. Wie der durch Emotet angerichtete Schaden eindrucksvoll belegt, können Cyber-Kriminelle mit Spear-Phishing-Methoden die erste Verteidigungs-Linie vieler Firmen durchdringen. Deren Netze liegen dann weitgehend offen vor den gierigen Fingern der Angreifer. Denn sie sind sicherheitstechnisch häufig weit hinter dem, was man eigentlich erwarten würde. Da finden sich oft reihenweise veraltete Systeme mit bekannten Sicherheitslücken. Von systematischen Vorkehrungen gegen den Klau von Passwörtern und Hashes kann keine Rede sein; Zweifaktor-Authentifizierung ist für die meisten Kleinunternehmen ein Fremdwort.

Böse Aussichten für 2019

Zwar hat sich der Einsatz von Antiviren-Software weitgehend durchgesetzt. Doch durch den Einsatz der mächtigen Windows PowerShell operieren die Kriminellen weitgehend unter deren Radar. So kann etwa PowerShell Empire über das Modul `InvokeMimikatz` den berüchtigten Passwort-Dieb direkt in den Arbeitsspeicher laden und dort ausführen. Zu keinem Zeitpunkt landet der verdächtige Mimikatz-Code auf der Festplatte, wo ihn ein Virenwächter entdecken könnte.

Der großflächige Einsatz dieser fortgeschrittenen Angriffstechniken durch Cyber-Kriminelle ist absehbar. Damit kommt auf alle Firmen eine neue Art von Angriffen zu. Deren wichtigster Baustein ist Dynamit-Phishing, dessen Qualität 2019 alle bisherigen Spam-Mails in den Schatten stellen wird. Beim Schutz davor helfen erste Maßnahmen wie die im nächsten Artikel geschilderten. Letztlich müssen aber sowohl die Mitarbeiter besser informiert als auch das Sicherheitsniveau der IT-Infrastruktur angehoben werden, um CyberCrime zu bändigen und wirklich verheerende Schäden zu verhindern. *(ju@ct.de)* c't

Schutzmaßnahmen gegen Emotet&Co: ct.de/y43u



Aus Emotets-Trickkiste: Wer nicht ganz genau hinschaut, sieht in Outlook nur die gefälschte Absenderadresse der Kanzlerin. Das echte „ju@..." ließe sich leicht aus dem Blickfeld schieben.

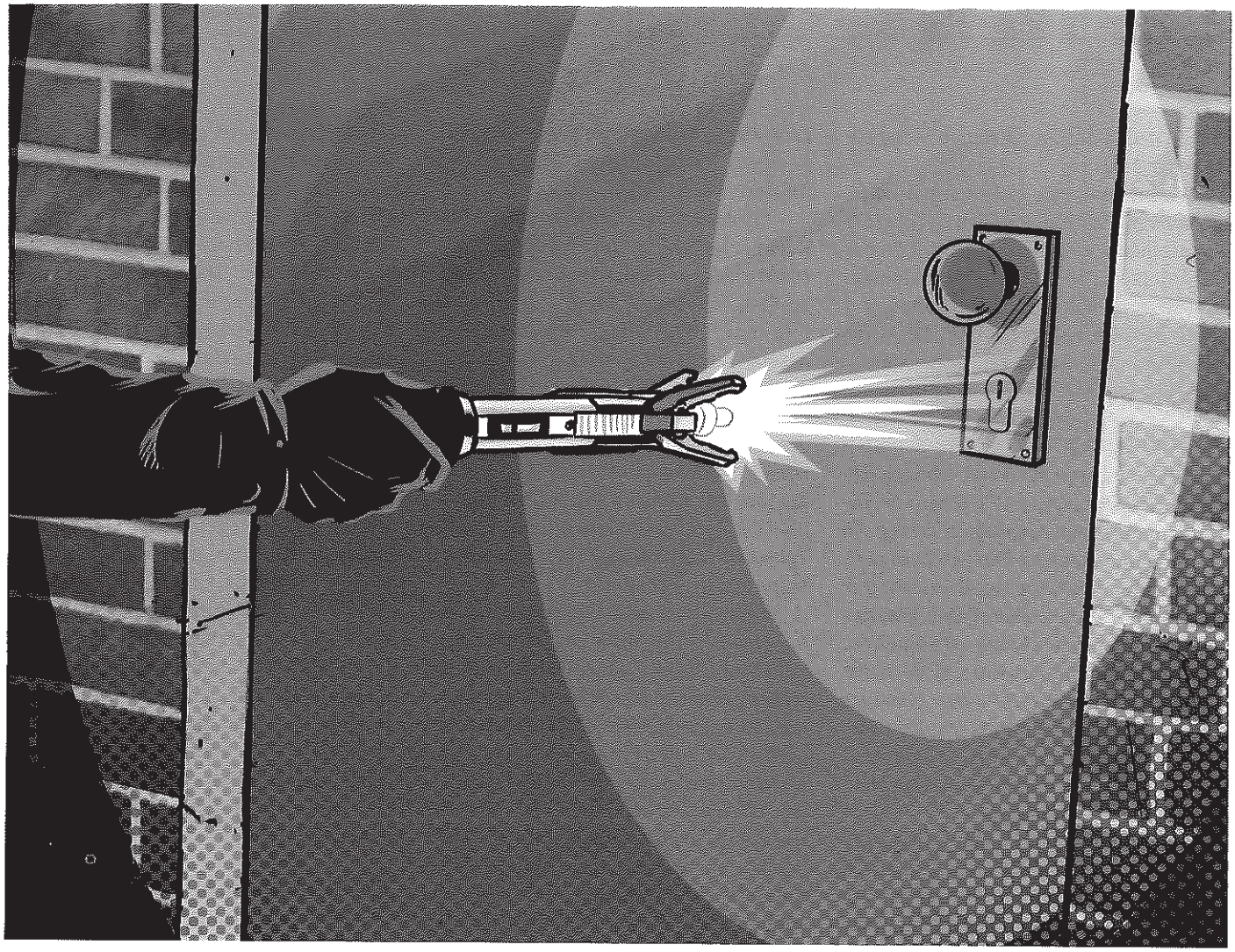


Bild: Albert Hulm

Dynamit-Phishing abwehren

So schützen Sie sich vor Emotet & Co.

Der Trojaner Emotet legt auch in Deutschland ganze Unternehmen lahm. Andere werden seinem Beispiel folgen. Bei vielen Firmen und Privatpersonen besteht deshalb akuter Handlungsbedarf.

Von Dennis Schirrmacher und Jürgen Schmidt

Das wichtigste Einfallstor für aktuelle Trojaner ist E-Mail. Deshalb sollte man bei Dateianhängen und Links immer vorsichtig sein – das gilt ganz allgemein und nicht nur bei radebrechenden Mails von Fremden. Trojaner wie der Windows-Schädling Emotet verbreiten sich mittlerweile oft über gefälschte Mails, die aussehen, als kämen sie von Freunden, Geschäftspartnern oder dem eigenen Chef. Diese Mails sind sehr gut gemacht und wirken aufgrund legitimer Absenderadressen und fehlerfreiem Deutsch sehr glaubhaft.

Firmen sollten deshalb ihre Mitarbeiter im sicheren Umgang mit Mails schulen und unterweisen. Emotet arbeitet mit angehängten Office-Dokumenten; häufig sind es angebliche Rechnungen im Doc-Format von Microsoft Word. Eine gute Regel ist es, vor dem Öffnen solcher Dateien beim angeblichen Absender kurz nachzufragen, ob das seine Richtigkeit hat. Das kostet wenig Zeit und kann viel Unheil verhindern. Und es ist definitiv keine Schande, sich bei einer möglichen Emotet-Mail nicht ganz sicher zu sein.

Admins können auch technische Maßnahmen ergreifen, um die Erkennung von Malspam zu erleichtern. Emotet missbraucht etwa den Anzeigenamen des Absenders, um dort eine vorgetäuschte Mail-Adresse zu platzieren. Im Anzeigenamen hat jedoch weder das @-Zeichen noch die eigene Mail-Domain etwas zu suchen. Nach beiden kann man eingehende Mails auf dem Mail-Gateway durchsuchen und entsprechend als möglichen Malspam markieren. Das komplette Ausfiltern von Office-Dateien ist hingegen eine drastische Maßnahme, die in der Praxis viel Ärger verursachen dürfte.

Makro-Viren abwehren

Die eigentliche Infektion erfolgt normalerweise nicht gleich beim Öffnen des Dokuments. Sie erfordert das Ausführen von Makros. Dabei handelt es sich um Befehlsketten, um etwa Layoutaufgaben zu automatisieren oder Berechnungen in Tabellen durchzuführen. Die Emotet-Autoren nutzen die Befehle jedoch dafür, Schadsoftware aus dem Internet nachzuladen und zu installieren.

Standardmäßig sind Makros in Microsoft Office deaktiviert. Sie lassen sich jedoch mit einem Mausklick auf „Inhalt aktivieren" recht einfach einschalten. Und die Malware-Autoren tun natürlich ihr Möglichstes, den Anwender zu diesem Schritt zu verleiten. Doch normalerweise benötigt man für ein Dokument, das via Mail ankommt, keine Makros. Wenn eine Datei aus einer Mail das Aktivieren von Makros einfordert, handelt es sich sehr häufig um einen Trojaner.

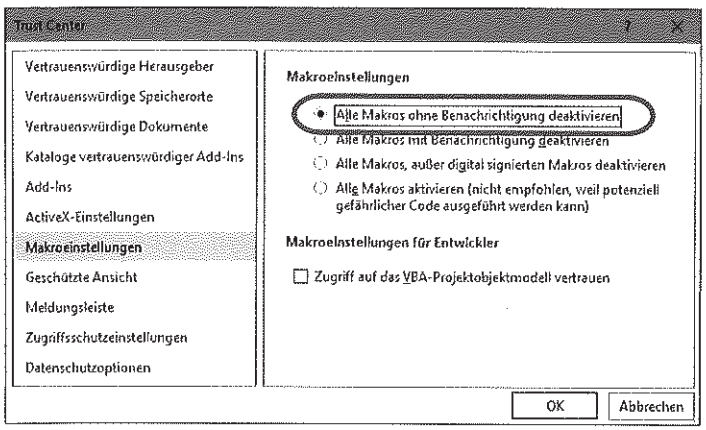
Die Makro-Einstellungen findet man beispielsweise in Office 2016 unter „Datei/Optionen/TrustCenter/Einstellungen für das Trust Center/Makroeinstellungen". Wer selbst nicht mit Makros arbeitet und diese nicht für den eigenen Workflow benötigt, sollte die sichere Variante „Alle Makros ohne Benachrichtigung deaktivieren" wählen. Dies kann aber die Arbeitsfähigkeit etwa beim Hantieren mit Tabellen deutlich beeinträchtigen, sollte also mit Bedacht umgesetzt werden. Admins in Unternehmen können die Makro-Verwendung unter Windows bequem über eine Gruppenrichtlinie reglementieren. Sie sollten den Gebrauch dieser gefährlichen Funktion soweit sinnvoll möglich verbieten.

In LibreOffice und OpenOffice funktionieren die Emotet-Makros nach jetzigem Kenntnisstand nicht. Ohne Makros können aktuelle Emotet-Varianten das System nicht infizieren. Andere Trojaner verwenden jedoch andere Tricks und auch die Emotet-Gang kann jederzeit eine neue Version etwa mit Schadprogrammen in ZIP-Archiven in Umlauf bringen. Verlassen Sie sich deshalb nicht ausschließlich auf diesen Schutz.

Basisschutz für Windows

Was für viele Computernutzer selbstverständlich ist, ist offensichtlich immer noch nicht Konsens: Ein Windows-Computer muss immer auf dem aktuellen Sicherheitsstand sein, damit er bestmöglich vor Trojanern geschützt ist. Checken Sie jetzt die Windows-Update-Funktion und prüfen Sie, ob auf Ihrem Computer alle aktuellen Sicherheitspatches installiert sind. Die Update-Pflicht gilt natürlich auch für alle anderen Anwendungen, wie insbesondere E-Mail-Clients und Webbrowser.

Ein wichtiges Sicherheitskonzept in Windows ist die Trennung zwischen Administratoren und eingeschränkten Nutzern. Während Erstere das System verwalten und etwa auch neue Software installieren dürfen, sind die Rechte für normale Nutzer reduziert. Das beschränkt auch den Schaden, den eine Malware auf dem System und im Netz anrichten kann. Insbe-



Das komplette Abschalten von Makros bietet den höchsten Schutz, bringt aber natürlich auch Einschränkungen mit sich.

sondere für Arbeitsplätze in Firmennetzen sollte man unbedingt Accounts mit eingeschränkten Rechten anlegen und nutzen.

Außerdem sollte man in Firmenumgebungen die Benutzerkontensteuerung (UAC) von Windows auf die höchste Stufe einstellen. Standardmäßig steht die auf „Mittel" und lässt sich damit leicht umgehen. In der höchsten Stufe verlangt Windows immer eine Bestätigung des Nutzers, wenn etwa ein Prozess mit Administrator-Privilegien ausgeführt werden soll. Sie finden die Einstellungen durch Eingabe von „UAC" im Suchfeld, das sich mit der Windows-Taste öffnet.

Unter Windows sollte man einen aktiven Virenwächter mit aktuellen Signaturen betreiben. Für den Grundschutz genügt der Windows Defender, den Windows 10 gleich mitbringt und der ab Werk aktiv ist. Allerdings sollte man sich nicht blind auf den Schutz der Antiviren-Software verlassen – ganz gleich welcher Marke. Die Erfahrung zeigt, dass es Cyber-Kriminellen immer wieder gelingt, deren Schutzfunktionen zu umgehen. Ein Virenwächter ist nur ein Baustein in einem guten Sicherheitskonzept.

Weitere Möglichkeiten, den Schutz zu erhöhen, sind Software Restriction Policies (SRP), die Separierung von Netzen und die Beschränkung des Powershell-Einsatzes. SRP können Sie bequem mit dem kostenlosen c't-Tool Restric'tor konfigurieren. Mehr Informationen zu vorbeugenden Schutzmaßnahmen gibt es etwa beim BSI für Bürger und speziell für Firmen bei der Allianz für Cybersicherheit. Alle Tipps und Tools finden Sie über ct.de/y1ck.

Kein Backup, kein Mitleid

Im Gefolge einer Infektion kommt oft weitere Schad-Software auf den Rechner – nicht selten ist das dann ein Erpressungstrojaner, der wichtige Daten verschlüsselt. Am besten ist man aufgestellt, wenn man seine Daten regelmäßig als Backup sichert. In Firmen sollte man das mehrmals täglich machen. Sollten Sie noch kein Backup haben, fangen Sie jetzt damit an! Wie man mit wenigen Handgriffen eine effektive und sogar automatisierte Backup-Strategie erstellt, zeigt ein kostenloser c't-Artikel (ct.de/y1ck).

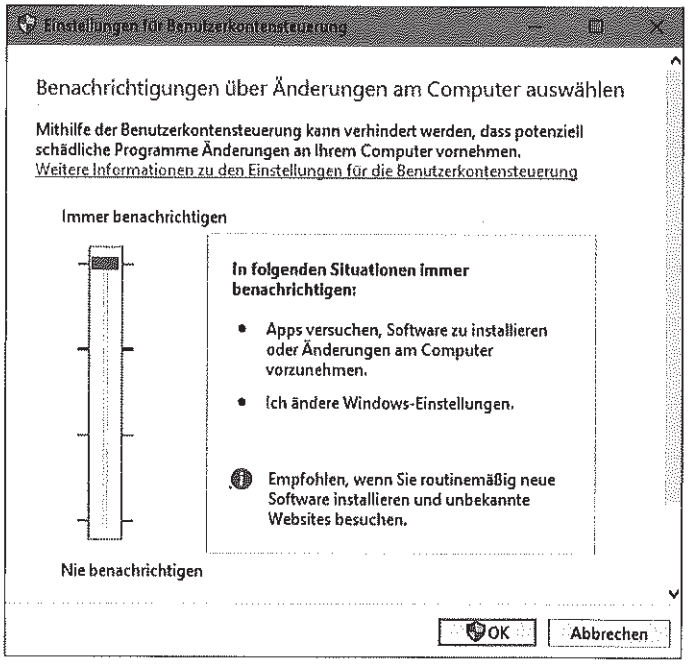
Hat Emotet zugeschlagen, sollte man alle infizierten Rechner neu aufsetzen und mit Hilfe der Backups wiederherstellen. Doktern Sie nicht an den Symptomen herum, bis der Rechner wieder sauber scheint. Emotet nimmt nicht nur selbst viele Veränderungen am System vor; er ist darauf spezialisiert, weitere Malware nachzuladen und zu installieren. Sie wissen also nie genau, was noch alles auf dem Rechner gelandet ist.

Darüber hinaus hat Emotet sehr ausgeklügelte Methoden, Informationen und speziell Passwörter zu stehlen. So nutzt es teilweise öffentlich verfügbare Tools wie WebBrowserPassViews und Mail PassView, um gespeicherte Passwörter aus dem System und Applikationen auszulesen. Außerdem versucht es auch, das Netzwerk-Passwort der am System angemeldeten Nutzer zu ermitteln. Betrachten Sie also alle auf dem System zum Einsatz kommenden Passwörter als kompromittiert und wechseln Sie diese so schnell wie möglich.

Und schließlich versucht Emotet sich mit den gestohlenen Zugangskennungen, einem Wörterbuch aus häufig genutzten Passwörtern und dem EternalBlue-Exploit auf Netzwerk-Freigaben zu verbinden und über diese auch weitere Systeme im Netz zu infizieren. Nehmen Sie also infizierte Systeme unverzüglich vom Netz, um eine weitere Ausbreitung zu verhindern. Melden Sie sich auch möglichst nicht mit privilegierten Accounts auf einem infizierten System an. Das könnte die weitere Ausbreitung des Schädlings beschleunigen.

Opfer sollten in jedem Fall Anzeige erstatten. In vielen Bundesländern kann man das sogar online erledigen. Betroffene Firmen können sich derzeit an die Zentrale Ansprechstelle Cybercrime für die Wirtschaft (ZAC) der einzelnen Bundesländer wenden und erhalten dort Hilfe. Privatpersonen erhalten zwar keine Unterstützung, aber zumindest Beratung. Ansprechpartner gibt es in jeder örtlichen Polizeidirektion in der Abteilung für Cyber-Kriminalität. *(des@ct.de)* c't

***Anleitungen:* ct.de/y1ck**



Die höchste Einstellung unterbindet Tricks von Schädlingen, die sich an der Benutzerkontensteuerung vorbeimogeln.