HORNETSECURITY

ADVANCED THREAT PROTECTION

WHITEPAPER

Whitepaper ..... Fehler! Textmarke nicht definiert.
Whitepaper ..... Fehler! Textmarke nicht definiert.
1 Problemstellung Advanced Threats 3
1.1 Einleitung 3
1.2 Klassifikation der neuen Angriffsvektoren 5
1.2.1 CEO-Fraud 5
1.2.2 Ransomware 6
1.2.3 Social Engineering und digitale Spionage 6
1.2.4 Spearphishing, Targeted Attacks 7
1.3 (Cyber) Kill Chain als Prototyp komplexer Cyberangriffe 7
1.4 Betriebsbeeinträchtigungen und Krisenreaktionen 9
1.5 Forensik und Wiederherstellung 10
2 Hornetsecurity Advanced Threat Protection 12
2.1 Funktionsweise der Analyse-Engines 12
2.2 Sandbox Engine 12
2.3 URL Rewriting 14
2.4 URL Scanning 15
2.5 Freezing 15
2.6 Targeted Fraud Forensics 16
2.7 Real Time Alert 16
2.8 Ex-Post-Alarmierung 18
2.9 ATP Report 19
3 Weitere Leistungen und Services 20
3.1 Spamfilter 20
3.2 E-Mail-Archivierung (Aeternum) 21
3.3 E-Mail Verschlüsselung 21
3.4 E-Mail Continuity 22
4 Quellen 23

1 Problemstellung Advanced Threats

1.1 Einleitung

Die Bedrohungsszenarien im Bereich E-Mail-Sicherheit haben sich in den vergangenen Jahren dramatisch verändert. Während Angreifer früher ihren Erfolg vor allem über massenweisen Versand relativ primitiv gemachter Spam-E-Mails suchten, ist heute eine starke Professionalisierung zu beobachten. Die „Machart" der Schad-E-Mails ist schwieriger erkennbar und wesentlich besser auf ihre Ziele und Opfer zugeschnitten. Herkömmliche Abwehrmethoden sind gegen diese Abgriffe weitgehend wirkungslos. Es sind neue Lösungen erforderlich.

In früheren Jahren setzten Angreifer auf Masse – je mehr Spam sie absenden konnten, desto größer war die Wahrscheinlichkeit, dass einige Spammails die Filter passierten und die Angreifer ihr Ziel erreichten. Im Jahr 2008 erreichte die Welle mit 99,7% des Spamverkehrs einen geradezu dramatischen Höchststand.

Die enormen Mengen an Spam verursachten allein durch belegte Leitungen, überquellende Mailboxen und Mailserver an der Lastgrenze erhebliche wirtschaftliche Schäden. Diese Schäden riefen konzertierte Aktionen zur Abwehr hervor – berühmt wurde unter anderem die Abschaltung des Providers McColo im November 2008, der zu einem deutlichen Abfall der Spamlevel führte. Auch wenn die betroffenen Botnetze damals schnell wiederaufgebaut wurden, wurde eines deutlich: Die Spammer schadeten sich durch die übergroßen Mengen an Spam letztlich selbst. Der Anteil an Spam im Mailverkehr ist seitdem rückläufig (Abbildung 1).

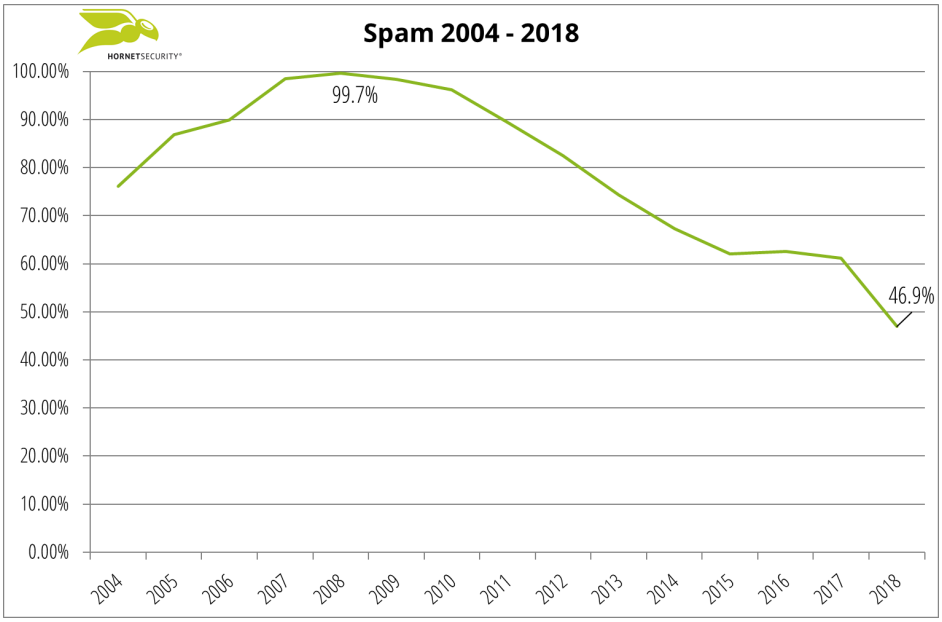

Abbildung 1: Entwicklung des Spamanteils im E-Mail-Verkehr 2004 – Mai 2018 (Quelle: Hornetsecurity)

Gleichzeitig sind die Angriffe aggressiver geworden, was am erhöhten Anteil an Viren in E-Mails sichtbar wird (Abbildung 2). Auch das Angriffsziel der per E-Mail verbreiteten Viren hat sich verändert: Ging es in früheren Jahren oft lediglich darum, einen Rechner zu kapern, um ihn zum Teil eines Botnets machen zu können, gehen die Angreifer jetzt direkter vor.

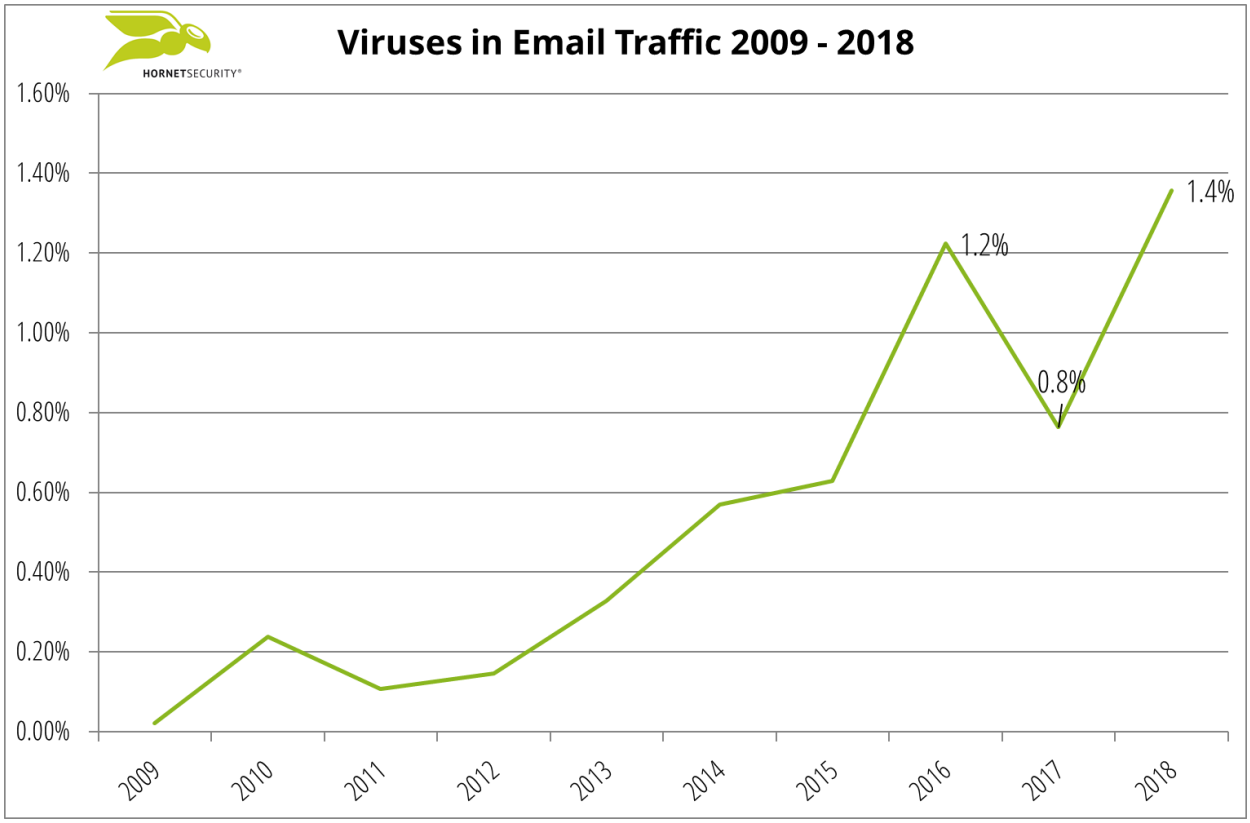

Abbildung 2: Viren im E-Mail-Verkehr 2009 – Mai 2018 (Quelle: Hornetsecurity)

Die Zahl an Ransomware-Angriffen hat in den letzten Jahren stark zugenommen (Abbildung 3) und mit Attacken wie Locky, GoldenEye und WannaCry große Schäden angerichtet.

Aber auch noch andere Angriffs-Szenarien sind im Laufe der Zeit angestiegen. CEO-Fraud und Spyware bedrohen die Integrität der IT-Infrastrukturen und die Sicherheit von Daten. Dies erhöht den Druck auf Betreiber und Nutzer von IT-Systemen deutlich, da neue Strategien nötig werden, um Systeme und Daten auch weiterhin effektiv zu schützen.

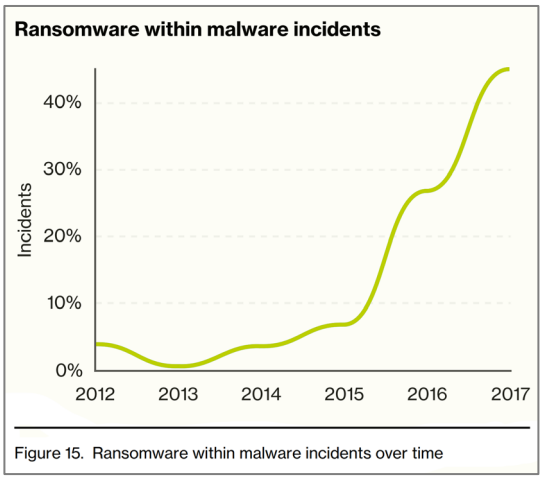

Abbildung 3: Anstieg von Ransomware-Angriffen (Quelle: 2018 Data Breach Investigations Report, Verizon)

1.2 Klassifikation der neuen Angriffsvektoren

Diese ausgeklügelten Angriffsmethoden stellen die IT-Security-Unternehmen vor etliche neue Herausforderungen. Viele der Angriffe lassen sich klassifizieren, manche Cyberattacken hingegen entziehen sich einer Einordnung, da sie häufig mehrere Komponenten gleichzeitig nutzen. Dennoch ist eine grobe Unterteilung der neuen Bedrohungen sinnvoll, um grundlegende Strategien zu erkennen und mögliche Abwehrmaßnahmen zu entwickeln. Einige dieser Methoden sollen etwas genauer beleuchtet werden:

1.2.1 CEO-Fraud

Bei CEO-Fraud, im Deutschen auch unter dem Begriff "Chefmasche" bekannt, schlüpfen Angreifer in die Identität von meist hochrangigen Mitarbeitern eines Unternehmens. Dabei handelt es sich häufig um Personen aus der Führungsebene (daher der englische Begriff „CEO" für „Geschäftsführer"), aber durchaus auch um andere weisungsbefugte Mitarbeiter wie Prokuristen oder Leiter der Finanzabteilung.

Die Angreifer senden gut gefälschte E-Mails an Mitarbeiter aus der Buchhaltung und versuchen, diese zur Überweisung von großen Geldbeträgen zu bewegen. Oftmals geschieht dies, indem die E-Mails einen starken Druck auf die Empfänger aufbauen, um eine schnelle Überweisung zu veranlassen. Um ihre Attacken möglichst realistisch zu gestalten, spähen die Angreifer vorab per Social Engineering ihre Opfer aus und verwenden Informationen über Vertragsverhandlungen oder Auslandsreisen. Weitere Ziele für die Angreifer können Kreditkartendaten oder Zugangsinformationen zu bestimmten Accounts sein.

Für klassische Antispam- oder Antiviren-Programme ist die Erkennung solcher E-Mails fast unmöglich. Der Grund: Sie beinhalten keine verdächtigen Dateianhänge, Links zu Schadseiten oder andere textlichen Hinweise, die sich Filtersysteme zu Nutze machen könnten. Außerdem werden die E-Mails individuell für jede Zielperson angefertigt und entziehen sich dadurch auch der Erkennung durch sehr häufiges Auftreten.

Diese Art von Angriffen hat in den vergangenen Jahren deutlich zugenommen. Auch wenn viele Betrugsversuche durch aufmerksame Mitarbeiter vereitelt werden konnten, entstehen erhebliche Schäden - in einem Einzelfall sogar 40 Millionen Euro. Laut der U.S. Bundespolizei FBI registrierte sie bis Mitte 2016 einen weltweiten Schaden von knapp 3,1 Mrd. US-Dollar.

1.2.2 Ransomware

Weltweit bekannt wurde Ransomware durch den Locky-Angriff, der im Februar 2016 viele Rechner und Netzwerke lahmlegte. Mittlerweile gibt es zahlreiche Nachfolger und Weiterentwicklungen, die immer wieder für Aufsehen und große Schäden sorgen. Bei Ransomware handelt es sich um Malware, die lokale Daten oder auch ganze Netzwerke verschlüsselt, um anschließend Lösegeldforderungen zu stellen. Oftmals ist die Schadsoftware als Rechnung oder Bewerbung getarnt und wird durch ein Makro in einer Textdatei oder Excel-Tabelle nachgeladen.

Dem Geschädigten bleibt anschließend keine Zeit mehr, um Gegenmaßnahmen durchzuführen. Es erscheint vielmehr auf dem Bildschirm ein Hinweis, dass die Daten verschlüsselt wurden und nun eine Lösegeldzahlung zu erfolgen habe, um den Entschlüsselungscode zu erhalten. Die Bezahlung soll in der Regel in Bitcoins erfolgen, was deren Verfolgung durch Strafverfolgungsbehörden erheblich erschwert. Es ist jedoch auch bei Zahlung des Lösegelds mehr als zweifelhaft, ob die Opfer tatsächlich den Entschlüsselungscode erhalten. Es sind Ransomware-Viren im Umlauf, die Daten einfach nur löschen und nicht verschlüsseln – sie können gar nicht wiederhergestellt werden. Daher raten Experten durchweg von der Lösegeldzahlung ab.

1.2.3 Social Engineering und digitale Spionage

Unter Social Engineering oder auch digitaler Spionage wird das Erlangen von Geheimnissen oder anderen Informationen verstanden. Im Fokus stehen dabei vor allem Staaten, Organisationen und Unternehmen, aber auch einzelne Personen. Das Ziel dieser Angriffsform ist es, das gewonnene Wissen zum eigenen Vorteil einzusetzen - entweder um dieses Wissen selbst einzusetzen oder um die Daten zu verkaufen.

Die Spyware **Camolog** sammelt Login-Daten verschiedener Programme (Mail-Client, Browser, FTP- und Instant-Messenger-Clients) und Informationen über einen Keylogger. Dieses Wissen wird von den Angreifern entweder gewinnbringend verkauft oder für Folgeangriffe verwendet. Das Besondere von Camolog ist, dass die Malware hartnäckige Anti-Analysetechniken einsetzt, um die eigene Existenz zu verschleiern. Als Transportmedium dient eine Phishingmail-Kampagne. Im Anhang befindet sich anstelle eines Angebots ein RAR-Archiv, in dem sich eine .NET-Datei versteckt. Diese wiederum fungiert als Dropper für die eigentliche Spyware. Da die Verschleierungstechniken so erfolgreich sind, hilft hier nur eine Analyse in der Sandbox. Mittels Verhaltensmustern ist es möglich, unter anderem das verräterische Anlegen von Registry Keys im Windows Autorun zu erkennen.

Bei Social Engineering kommen verschiedene Methoden zum Einsatz: Neben klassischem Hacking und Datendiebstahl sammeln Angreifer mittlerweile etliche Informationen aus sozialen Netzwerken wie Twitter, Facebook und Co, um daraus Schlüsse für gezielte Attacken ziehen zu können (siehe auch CEO-Fraud).

1.2.4 Spearphishing, Targeted Attacks

Spearphishing-Attacken sind die Weiterentwicklung von Phishing-Angriffen. Zielen letztgenannte auf das Abschöpfen von Passwörtern oder anderen privaten Daten in einer allgemeinen Form ab (Phishing ist eine Wortkreation aus den englischen Begriffen „password" und „fishing"), ist Spearphishing auf einzelne Personen ausgerichtet. Durch eine persönliche Ansprache oder eine vermeintlich gemeinsame Vergangenheit bauen die „Spearphisher" eine direkte Vertrauensebene zum Opfer auf, um zu einem späteren Zeitpunkt an Passwörter, Zugangsdaten oder Bankverbindungen zu erlangen. Anschließend nutzen die Angreifer diese Informationen aus, um ihre Vorteile daraus zu ziehen. Zielt eine solche Attacke auf eine wichtige Person (siehe auch „CEO-Fraud"), spricht man auch von „Whaling" (Kombination aus „Whale" im Sinne von „dicker Fisch" und „Phishing").

1.3 (Cyber) Kill Chain als Prototyp komplexer Cyberangriffe

Wie ausgefeilt Angriffe auf Unternehmen vonstattengehen, lässt sich anhand der Kill Chain anschaulich verdeutlichen. Ursprünglich vom Rüstungsunternehmen Lockheed Martin aus dem militärischen Blickwinkel heraus entwickelt, lässt sich der schematische Ablauf gut auf den IT-Security-Bereich ausweiten.

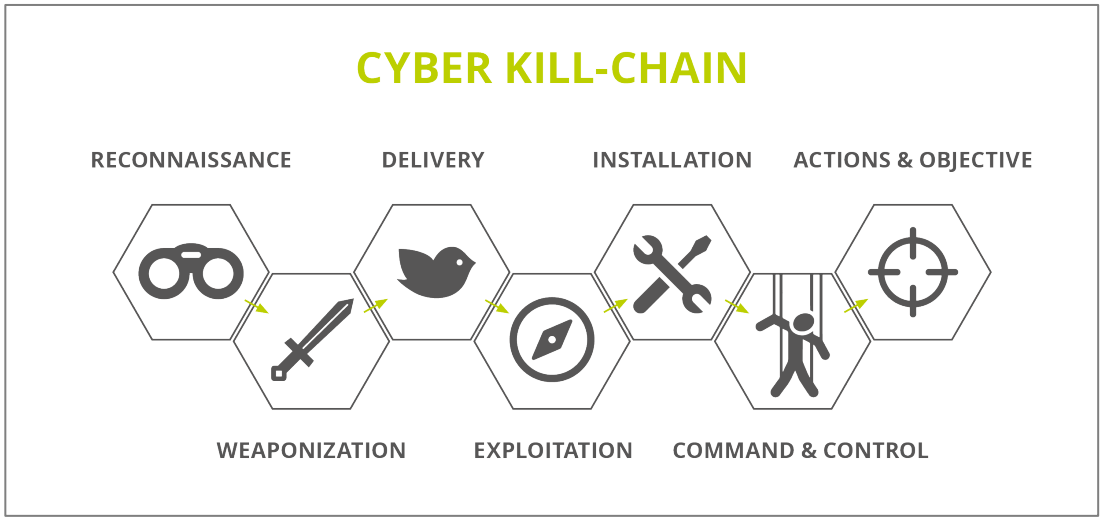

Abbildung 4: Schematischer Ablauf einer Kill Chain

Zunächst erweiterten die Entwickler von **Emotet** ihre *E-Mail-Adressdatenbank*, indem sie auf bereits infizierten Systemen mit Hilfe eines Moduls das Adressbuch von Microsoft Outlook auslasen. Anschließend *präparierten sie ein Microsoft Word- oder Excel-Dokument*, in dem sich ein Makro befand. Diese Datei war häufig als Rechnung getarnt, um unauffällig gegenüber dem Benutzer zu erscheinen und um die Öffnungsrate zu erhöhen. Mit Hilfe einer einfachen, aber effizient gestalteten *Phishing-E-Mail* wurde das Office-Dokument an die neu gewonnenen E-Mailadressen versendet. Mit diesen Mails versuchten die Angreifer, Benutzer dazu bringen, das angehängte Dokument zu öffnen und *das Makro zu aktivieren*. Sobald das Makro gestartet war, führte es einen PowerShell-Befehl aus, *lud „Emotet" nach und führte den Schadcode* aus. Um möglichst wenig Aufsehen zu erregen, aktivierte „Emotet" dabei zunächst wenige Funktionen. Später überwachte die Malware den Internetverkehr und *infiltrierte den Traffic beim Online-Banking*, um so Geld zu entwenden. Der Vorteil dieses Vorgehens war, dass die Cyberkriminellen jederzeit den downloadbaren Payload ändern konnten.

Das Konzept sieht insgesamt sieben Stufen vor, die von der Ausspähung der Opfer über die Ausnutzung einer Schwachstelle bis hin zum Abschluss des Angriffs reichen. Das Gute: Alle Angriffsschritte müssen erfolgreich sein, damit der Angreifer sein Ziel erreicht. Zur Abwehr reicht es, die Angriffskette an einer Stelle zu durchbrechen. Gelegenheit dazu gibt es an jeder Stufe des Angriffs, entsprechend ist eine vielstufige Abwehr sinnvoll, die jede Angriffsstufe adressiert. Dies erleichtert es erheblich, den Angriff wirkungsvoll zu stoppen. Idealerweise arbeiten außerdem die einzelnen Abwehrstufen zusammen und tauschen untereinander Informationen aus.

Seit 2014 existiert der Banking-Trojaner „Emotet" bereits, und immer noch findet er in leicht abgewandelten Variationen Anwendung bei Cyberangriffen. An diesem lässt sich exemplarisch die Cyber Kill Chain erklären (siehe auch Abbildung 4).

Neben Audits und regelmäßigen Sicherheitstests der eigenen Infrastruktur ist ein professionelles Patchmanagement, Abwehrmaßnahmen wie Spam- und Webfilter und schließlich eine umfassende Backup-Umgebung vonnöten.

Ein weiteres Argument für den Einsatz von verschiedensten Abwehrmaßnahmen ist, dass jeder Angriff anders aufgebaut ist. Über Verteidigungslinien für jede Stufe lässt sich die Wahrscheinlichkeit deutlich erhöhen, auch neuartige und noch unbekannte Angriffe zu unterbinden - verschiedene Abwehrmechanismen für verschiedene Angriffsarten. Durch die Kombination verschiedener Abwehrmaßnahmen wird die Gefahr eines Schadens erheblich gemindert.

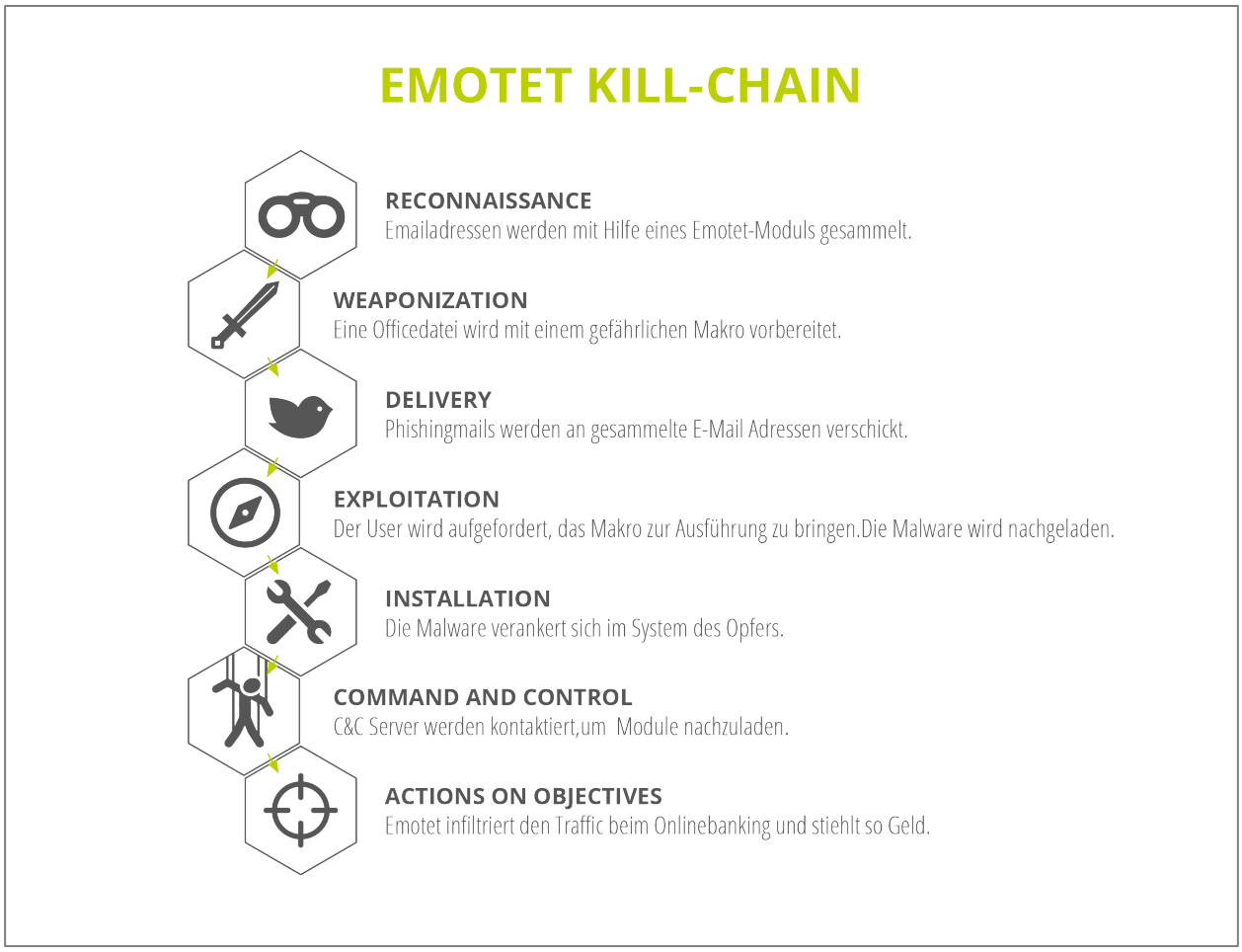

Abbildung 5: Kill-Chain-Angriff am Beispiel der Emotet-Malware

1.4 Betriebsbeeinträchtigungen und Krisenreaktionen

Was ist jedoch zu tun, wenn Angreifer erfolgreich in die IT-Infrastruktur eines Unternehmens eindringen konnten? In einem solchen Fall ist das primäre Ziel, den Schaden einzudämmen, beispielsweise durch umgehende Isolation oder Abschaltung betroffener Systemteile, um eine Ausbreitung innerhalb des Unternehmensnetzwerks zu minimieren. Zu bedenken ist jedoch, dass oftmals die Verbreitungswege noch unbekannt sind, so dass die Erfolgswahrscheinlichkeit der Schadenseindämmung gering ist. Zudem verursacht diese Maßnahme auch häufig Stillstände von Subsystemen, was wiederum Produktionsausfälle auslösen kann.

Im Anschluss an Maßnahmen zur Schadenseindämmung sollte eine Beurteilung der betroffenen Daten und Systeme stattfinden. Je nach Art des Angriffs können Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität von Daten oder auch Kombinationen dieser Gefährdungskategorien verletzt sein. (vgl. Sichere Nutzung von E-Mail (ISi-Mail-Client), BSI-Leitlinie zur Internet-Sicherheit (ISi-L), Version 1.0, Stand 22.03.2016.

Bei der Verletzung von Integrität und Authentizität werden Daten bewusst verändert oder gefälscht, um dem Angreifer durch Betrug einen wirtschaftlichen Vorteil zu verschaffen oder Fehlinformationen zu verbreiten. Attacken auf die Vertraulichkeit bedeuten eine Informationserlangung, beispielsweise von Passwörtern oder andere Wege der Industriespionage. Angriffe auf die Verfügbarkeit zerstören Daten entweder direkt oder verhindern einen nutzbaren Zugriff darauf (etwa durch Ransomware).

Das Schadensausmaß ist erheblich davon abhängig, welche technischen und organisatorischen Maßnahmen die betroffene Organisation in den Bereichen Prävention, Detektion und Reaktion getroffen hat.

Eine Auswertung aus 600 Rückmeldungen von Unternehmen aus der deutschen Wirtschaft durch das BSI ergab, dass zu 70 Prozent einzelne Arbeitsrechner befallen wurden, bei 22 Prozent kam es zu erheblichen Ausfällen der IT Infrastruktur und 11 Prozent erlitten einen dauerhaften Verlust wichtiger Daten. 2 Prozent der von Ransomware bereits betroffene Unternehmen gaben sogar an, dass durch die Ransomware-Infektion die wirtschaftliche Existenz gefährdet ist oder war.

1.5 Forensik und Wiederherstellung

Sind Daten verloren oder durch eine Attacke unbrauchbar geworden, so kann je nach Angriffsart nicht nur ein lokaler PC betroffen sein, sondern auch Netzlaufwerke, ganze Fileserver oder Teilbereiche von Rechenzentren. Ist ein Backup der nicht nutzbar gemachten Daten vorhanden, so lässt sich die Störung durch Einspielen des Backups verringern. Dies ist jedoch in jedem Fall mit einem Zeit- und möglicherweise einem Datenverlust verbunden, da zwischen dem Zeitpunkt des letzten Backups und dem Beginn der Datenvernichtung eine Lücke klafft.

Leider kann eine Wiederherstellung wichtige Informationen, die für die Forensik benötigt werden, zerstören, von daher kann auch eine Teilwiederherstellung sinnvoll sein, um mindestens ein betroffenes System in einem analysierbaren Schadzustand belassen zu können. Forensik ist nötig, um festzustellen, wo genau der Angreifer gewesen ist, welche Daten abgeflossen, gelöscht oder verändert wurden.

Für Analysten sind diese Informationen unabdingbar, um das tatsächliche Ausmaß des Schadens festzustellen; sie können jedoch auch aus Compliance-Sicht erforderlich sein (etwa zur Meldung an Behörden). Auch für die Öffentlichkeitsarbeit nach einem Security-Vorfall kann Forensik dazu dienen, um Ursache und Auswirkung präzise darzustellen und somit die Schäden einzugrenzen.

Das reine Einspielen von Backups ist daher nur begrenzt hilfreich, verhindert Forensik womöglich sogar, weil es die Spuren des Angreifers überschreibt. Deshalb kann Forensik auch die Wiederherstellung des Betriebszustands verzögern – so geschehen z.B. im Nachgang des Ransomware-Angriffs auf ein Krankenhaus in Neuss.

Die verschiedenen Schutzeinrichtungen helfen auch, wenn sie den Vorfall selbst nicht verhindert haben – weil sie nämlich Aktivitäten protokollieren und damit Forensik erst ermöglichen. Da die meisten Unternehmen und Institutionen jedoch nicht dokumentieren, wer welche Dateien wann ändert (oder verschlüsselt), ist etwa nach einem Ransomware-Angriff häufig ein enormer Aufwand nötig, um sicherzustellen, dass keine Daten verloren gegangen sind. Oftmals müssen ganze Fileshares gelöscht und durch Backups ersetzt werden. Bei einem Drittel der Betroffenen dauerte die Wiederherstellung länger als 48 Stunden

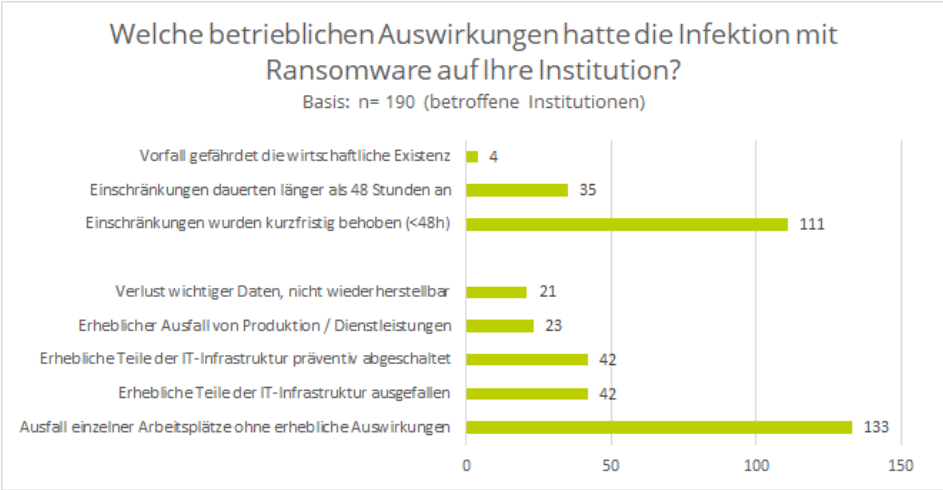

Abbildung 6: Betriebliche Auswirkungen einer Ransomware-Infektion (Quelle: BSI)

Neben dem Produktivitätsausfall und den Aufwendungen für Forensik und Wiederherstellung haben die Unternehmen einen weiteren Schaden zu verkraften, der monetär schwer messbar ist, aber dennoch enorme Ausmaße annehmen kann – den Reputationsverlust. Denn im Fall eines Datenverlusts ist dies zuständigen Behörden sowie den Betroffenen unverzüglich zu melden. Dies kann sogar dazu führen, dass bei Datenschutzverletzungen eine Veröffentlichung auf Webseiten oder in großen Tageszeitungen vom Gesetzgeber vorgegeben ist. In solchen Fällen müssen betroffene Unternehmen namentlich genannt werden und diese wiederum Stellung zum Vorfall beziehen.

Ein weiterer Punkt: Vielfach haftet das Unternehmen für Fremdschäden, die durch den Angriff entstanden sind, entsprechend seinen vertraglichen Verpflichtungen gegenüber den Geschäftspartnern. Auch dann sind genaue Informationen über den Hergang und die Auswirkungen des Angriffs wichtig.

Aufgrund der möglicherweise verheerenden Auswirkungen und der Vielzahl an Angriffsszenarien ist es sinnvoll, den Schutz der Infrastruktur mehrdimensional und an der frühestmöglichen Stelle anzusetzen: So ist für einen erfolgreichen Schutz entscheidend, alle Kommunikationswege zu schützen. Heutige Angriffe sind inzwischen so vielseitig aufgebaut, dass eine reine Absicherung zum Beispiel nur des E-Mail-Verkehrs nicht ausreicht.

Eine Aufklärung der Endbenutzer ist ebenfalls zwar grundsätzlich richtig und wichtig, aber kein ausreichender Schutz, da viele Attacken im E-Mail- und Webbereich inzwischen so professionell aufgebaut sind, dass Menschen sie kaum mehr von gültigen Nachrichten oder Webseiten unterscheiden können. Zudem sind in Zeiten mobiler Arbeitsumgebungen rein stationäre Lösungen, die das Unternehmen physikalisch von der Außenwelt abschotten, überholt. Vielmehr ist es empfehlenswert, eine Security-Ebene vorzuschalten, welche die Unternehmenskommunikation mehrdimensional absichert und das Unternehmen aktiv vor Bedrohungen schützt.

Gerade in Zeiten von Zero-Day-Exploits ist es für Unternehmen wichtig, bei solchen Security-Ebenen auf die Fähigkeit der Erkennung ab der ersten Mail einer Angriffswelle zu achten.

2 Hornetsecurity Advanced Threat Protection

Mit seiner Lösung hat Hornetsecurity ein Produkt auf den Markt gebracht, das die oben genannten Bedrohungen zuverlässig von der IT-Infrastruktur seiner Kunden fernhält. Dabei setzt Hornetsecurity wie bei all seinen anderen Services auf die Cloud-Technologie.

2.1 Funktionsweise der Analyse-Engines

Hornetsecurity verwendet diverse hochinnovative Analyse-Engines, die komplexe Attacken in Echtzeit erkennen und sofort unterbinden. Gleichzeitig liefert der ATP-Report detaillierte Informationen über die Angriffe auf die Ziel-Unternehmen.

Nachfolgend sind in diesem Dokument die wichtigsten Hintergrundinformationen zur Funktionsweise der Erkennungs-Engines von Hornetsecurity Advanced Threat Protection (ATP) zusammengefasst.

2.2 Sandbox Engine

Klassische Anti-Viren-Lösungen erkennen Schadprogramme an ihrer Gestalt – genauer an bestimmten Datensequenzen. Moderne Schadprogramme umgehen diese Erkennung, indem sie ihre Gestalt immer wieder sehr schnell verändern. Eine andere Erkennungsmethode setzt daher auf die Erkennung des Verhaltens eines Programms. Deshalb ist es ratsam, E-Mail-Anhänge aus unbekannten Quellen vorher in gesicherten Systemumgebungen zu starten. Die Sandbox-Engine übernimmt diese Aufgabe automatisiert (Abbildung 6).

Nach der Ausführung des potenziell schädlichen Dateianhangs analysiert die Sandbox alle Systemveränderungen. Dies kann das Verhalten der Systemprozesse sein, Systemaufrufe, Zugriffsversuche auf die System-API oder Veränderungen an der Registry. Anschließend erfolgt ein Abgleich mit bekannten Verhaltensmustern und bei Übereinstimmungen ein Blockieren der Träger-E-Mail.

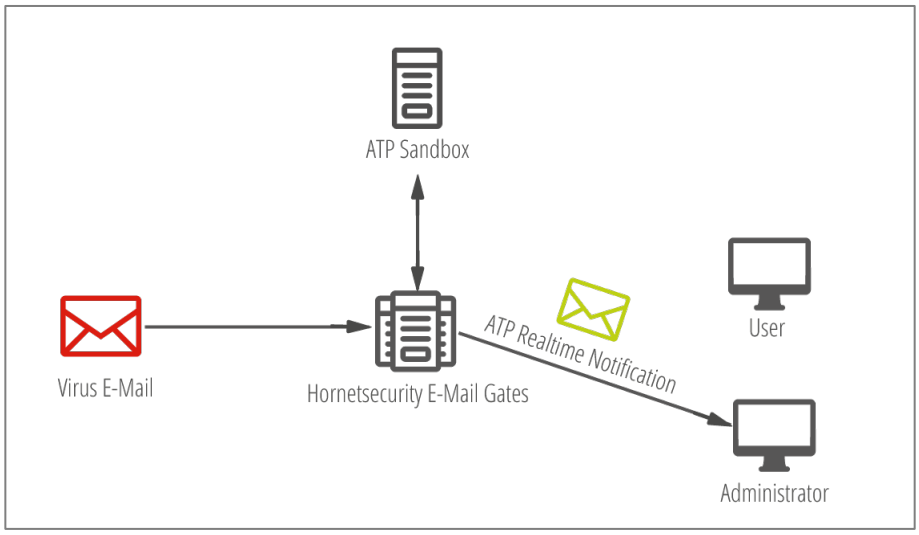

Abbildung 7: Sandbox Engine

Zusätzlich schneidet die Sandbox den gesamten Netzwerkverkehr des Systems mit. Ein Beispiel: Die untersuchte Datei versucht, mit einem Command-and-Control-Server zu kommunizieren, um so heimlich Schadcode nachzuladen. Die Sandbox erkennt solch auffällige Verbindungen, die ein Indikator für Malware sein können, und stoppt die Zustellung der schädlichen E-Mail. Von allen Aktivitäten der Datei erstellt die Sandbox-Engine automatisch Screenshots, die anschließend in den ATP-Report aufgenommen werden. Aus Basis all dieser Analysen nimmt anschließend die Sandbox-Engine eine Gefahrenabschätzung vor. Hierfür vergibt sie unter Verwendung einer multikriteriellen Bewertungsfunktion einen Wert zwischen 0 (ungefährlich) und 10 (hochgefährlich). Dieser Wert erscheint zudem in den ATP-Report als Score.

Der Remote Access Trojaner **Nanocore** ist eine bereits seit Jahren bekannte Malware, die auch bereits sehr ausführlich analysiert ist. Dennoch ist sie immer noch im Einsatz, da sie im Erfolgsfall sehr gefährlich für das Opfer werden kann: Nanocore erlaubt es den Angreifern, die infizierten Systeme komplett aus der Ferne zu steuern und zu überwachen. Aufgrund des bekannten Schadcodes selbst ist die Verschleierung der Auslieferung besonders wichtig. So verwendet Nanocore eine Mischung aus Phishing-Mail, einem Winrar-Archiv und einem frei nutzbaren Admintool AutoIT. Die Malware verriet sich durch die Verhaltensanalyse der Hornetsecurity Sandbox, die unter anderem das Entpacken des Dateiarchivs und das Erstellen neuer Dateien erkannte, aber auch auf die Modifikation von Registryeinträgen und auffällige Netzwerkkommunikation stieß.

Nach Abschluss der dynamischen Analyse wird die Sandbox-Umgebung automatisch wieder in ihren Ausgangszustand zurückversetzt, um Auswirkungen früherer Analysen zu beseitigen und für die kommenden Untersuchungen eine möglichst authentische Umgebung bereitzustellen.

Darin enthalten sind umfangreiche Informationen wie die Gefährlichkeitsbewertung, die angefertigten Screenshots sowie die Verhaltenssignaturen, die zum Einsatz kamen (siehe Abschnitt „ATP-Report“).

Nach Abschluss der Sandbox-Analyse gleicht Hornetsecurity ATP den E-Mail-Anhang mit den Signaturen von 25 verschiedenen klassischen Anti-Viren-Engines ab. Anschließend stehen alle Analyseergebnisse zur Datei strukturiert im ATP-Report zur Verfügung Darin enthalten sind umfangreiche Informationen wie die Gefährlichkeitsbewertung, die angefertigten Screenshots sowie die Verhaltenssignaturen, die zum Einsatz kamen (siehe auch Kapitel 2.9 "ATP-Report").

Da dieses Vorgehen auch den Angreifern bekannt ist, prüfen aktuelle Viren bei der erstmaligen Ausführung Registry- und BIOS-Einträge auf eine mögliche virtuelle Umgebung. Falls dies der Fall ist, findet keine Injektion des schädlichen Codes ins System statt. Die ATP-Sandbox-Engine ist in der Lage, solche Anti-VM-Maßnahmen zu erkennen, entsprechend zu bewerten und Schadcode auch darüber zu erkennen.

2.3 URL Rewriting

Bei Blended Attacks wird der eigentliche Schadcode oft über Webseiten nachgeladen, auf die eine URL in der verschickten E-Mail verweist. Um die Erkennung in E-Mail-Filtern zu umgehen, wird der Schadcode von den Angreifern dabei oft erst einige Stunden nach dem Versand der E-Mail hochgeladen. Die Filter im E-Mail-Strom können keinen Schadcode finden und lassen die E-Mail passieren. Erst wenn der Empfänger zu einem späteren Zeitpunkt die URL aktiviert, ist der Schadcode hinterlegt und wird ausgeführt.

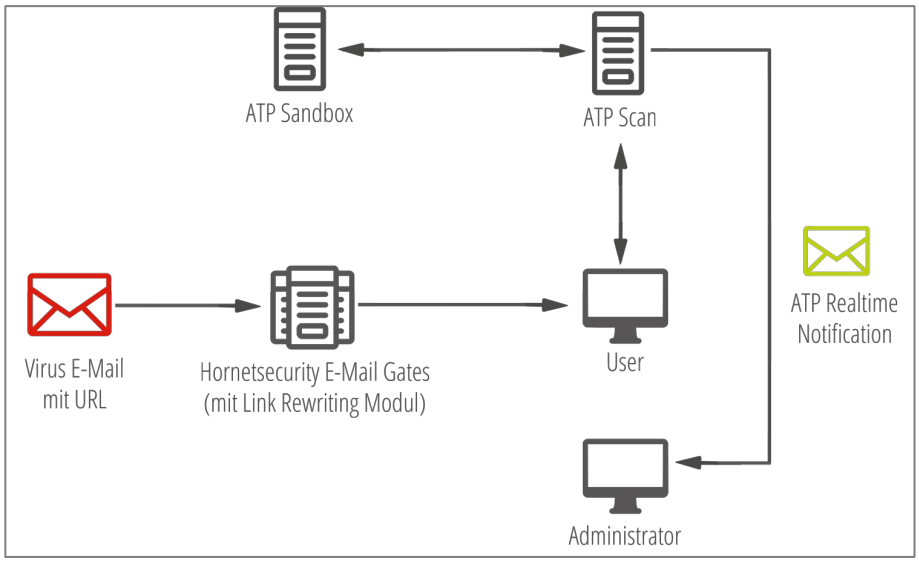

Abbildung 8: Funktionsablauf des URL Rewritings

Beim URL Rewriting werden deshalb Links in verdächtigen E-Mails umgeschrieben, sodass der Benutzer zum Zeitpunkt der Aktivierung eines Links in einer E-Mail über einen Hornetsecurity Webfilter abgesichert surft (Abbildung 8).

Dieser Webfilter analysiert den Netzwerkverkehr mithilfe von zwei Anti-Viren-Engines, einer Datenbank an Domain-Kategorisierungen und der ATP-Sandbox. Downloads muss der Benutzer zunächst prüfen,

bevor er sie anstößt. Dieses Vorgehen eliminiert die Gefahr, sich durch schädlichen Content via Weblinks zu infizieren, ohne dass Einstellungen am System des Benutzers vorgenommen werden müssen.

URL Rewriting ist eine optimale Ergänzung zum URL Scanner (siehe unten), da der URL Scanner keine Objekte (etwa Dokumente im Anhang) überprüfen kann, die erst beim Aufruf einer Webseite durch Skripte oder durch Benutzerinteraktionen dynamisch geladen werden.

2.4 URL Scanning

Das Feature URL Scanning von Hornetsecurity ATP ist ein zusätzliches Filtermodul, das ein weiteres Einfalltor für Malware schließt (Abbildung 9).

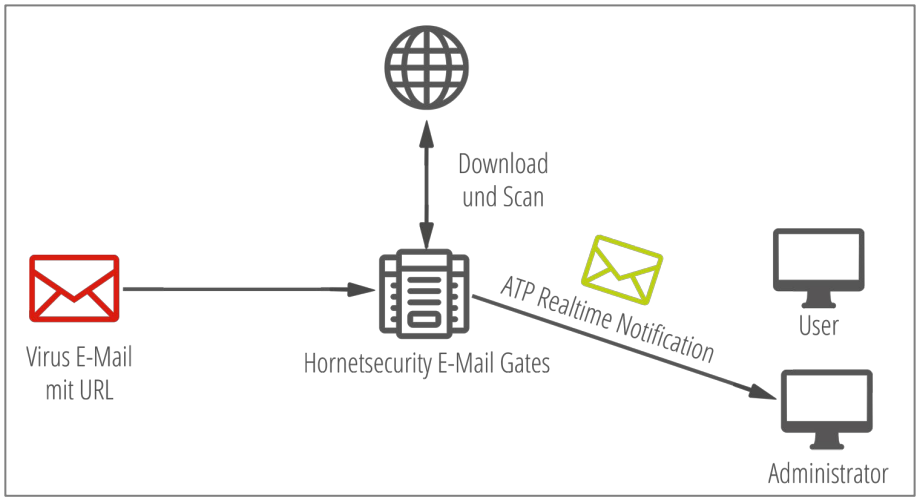

Abbildung 9: Ablauf beim URL Scanning

Der URL Scanner analysiert den Inhalt, auf den URLs in E-Mail-Attachments verweisen, mit diversen Anti-Viren Engines und heuristischen Filtern. Vorteil gegenüber URL Rewriting: Hornetsecurity ATP gewährleistet auf diese Art und Weise die Integrität von Dateianhängen und nimmt keine Änderung an der Datei selbst vor. Nachteil gegenüber URL Rewriting: Der URS-Scanner arbeitet zum Zeitpunkt der Übertragung der E-Mail. Wird der URL zu einem späteren Zeitpunkt Schadcode untergeschoben, ist der URL-Scanner wirkungslos dagegen.

2.5 Freezing

Hornetsecurity überprüft E-Mail-Anhänge mit mehreren Anti-Viren-Engines und heuristischen Filtern. Wird ein verdächtiger E-Mail-Anhang beim ersten Scanvorgang nicht als bösartig eingestuft, so unterbricht das ATP-Freezing die Zustellung der E-Mail für einen kurzen Zeitraum. Während dieser Zeit erhalten die Signaturen der Anti-Viren-Lösung von Hornetsecurity aktualisierte Daten. Nach Ablauf der Zeit wird die eingefrorene E-Mail mit den aktuellsten Signaturen erneut überprüft. So lassen sich Fehlkategorisierungen minimieren, zudem wird der Schutz vor Zero-Day-Exploits hierdurch optimal ergänzt.

2.6 Targeted Fraud Forensics

Professionelle Betrüger führen gezielte (Spear-)Phishing-Attacken per E-Mail durch. Im Visier stehen CEOs, Personal aus der Buchhaltung oder sonstige Mitarbeiter, die Zugriff auf Finanzen oder sensible Daten eines Unternehmens haben. Die Betrüger geben hierbei vor, eine andere Identität zu besitzen, um die Zielperson zu täuschen und zu einer Handlung zu veranlassen. Dies kann die Herausgabe von sensiblen Daten sein, aber auch die Überweisung einer bestimmten Summe auf ein fremdes Konto.

Der Abwehrmechanismus Targeted Fraud Forensics besteht aus einer komplexen Sammlung von Maßnahmen, die E-Mails auf Anzeichen von Finanzbetrug, Identitäts- und Informationsdiebstahl überprüfen:

- Das *Intention Recognition System* führt eine erste Analyse der E-Mail-Inhalte durch. Hierbei werden nicht nur die Inhalte des E-Mail-Bodys auf besondere Merkmale hin untersucht, sondern gegebenenfalls auch der Aufbau und die Attribute von E-Mail-Anhängen.
- Die *Identity Spoofing Recognition* erkennt auf Basis des E-Mail-Headers und der SPF-Records der Domain des E-Mail-Absenders, ob ein Identitätsdiebstahl vorliegt.
- Die *Spy-Out Detection* und *Feign Facts Identification* dienen als Spionage- und Betrugsabwehr von Attacken zur Erlangung sensibler Informationen. Hierbei werden E-Mails auf Signalwörter bzw. Strings untersucht, die Indiz für einen Betrugs- oder Spionageversuch sein können.
- Mit der *Targeted Attack Detection* lassen sich gezielte Angriffe auf einzelne Personen mithilfe von erweiterten Heuristiken erkennen und abwehren. Notwendig ist dazu, besonders exponierte Personen (z.B. CEO, Buchhaltung) vorab zu definieren.
- Durch die *Fraud Attempt Analysis* lässt sich die Authentizität und Integrität von Metadaten und Mailinhalten prüfen.

2.7 Real Time Alert

Hornetsecurity informiert seine Kunden in Echtzeit über blockierte Angriffe auf die IT Infrastruktur, die per E-Mail erfolgt sind. Wird ein Angriff abgewehrt, so erhalten die zuvor definierten Kontaktperson aus dem Kundenunternehmen einen sogenannten Real Time Allert (Abbildung 10) über die Angriffsart. In dieser sind weitere Informationen zur abgefangenen E-Mail zu finden, zum Beispiel Absender, Empfänger oder ob ein schadhaftes URL- oder E-Mail-Attachment mitgesendet wurde.

HORNETSECURITY®

Hornetsecurity Advanced Threat Protection - Real Time Alert

The Hornetsecurity Advanced Threat Protection Service has just detected the following email attack:

Classification:	Hornet-ATP03
User:	accounting@yourcompany.com
Date:	09/22/2016 12:09 PM CEST
Sender:	hacker@maliciousdomain.com, ceo@yourcompany.com
Server Address:	123.123.123.123, mail.hackedserver1237.com
Reason:	ATP Sandbox
Attachment:	payment_sheet.js

Abbildung 10: Real Time Alert

In der Benachrichtigung ist detailliert aufgeführt, welcher Erkennungsmechanismus die schädliche E-Mail an der Zustellung gehindert hat. Dies lässt wiederum genauere Rückschlüsse auf den Angriffsvektor zu.

Klassifizierung	Grund
atp-doc-inject	**ATP Document Obfuscated Injection Scanner** Mechanismen zur Analyse der Mailanhänge auf eingebettete verdächtige Inhalte.
atp-doc-link	**ATP Document Obfuscated Link Injection Scanner** Engine zur Analyse der Links in Mailanhängen auf das Nachladen verdächtiger Inhalte.
atp-doc-inject-heur	**ATP Document Injection Heuristic** Heuristische Filtergruppen zur Erkennung schadhafter Anhänge.
atp-html-content	**ATP HTML Content Attack Detection** Dynamische Analyse und Ermittlung verdächtiger Muster in HTML-Inhalten.
atp-url-archive	**ATP URL Archive Attack Detection** Erkennung von Links, über die Archive mit schadhaften Inhalten nachgeladen werden, wie sie beispielsweise in Blended Attacks vielfach verwendet werden.
atp-phish-domain	**ATP Phishing Domains** Identifikation von Domains, die bereits in Zusammenhang mit Phishing in jüngster Vergangenheit auffällig waren, beispielsweise durch gehackte Websites.

atp-sandbox	**ATP Sandbox Analyses** Dateianhänge werden in einer Vielzahl verschiedener Systemumgebungen ausgeführt und ihr Verhalten analysiert. Stellt sich heraus, dass es sich um Malware handelt, wird der Nutzer benachrichtigt. Schützt vor Ransomware und Blended Attacks.
atp-ff-spy-out	**ATP Fraud Forensics: Spy Out Detection** Spionageabwehr von Attacken zur Erlangung schützenswerter Informationen.
atp-ff-identity	**ATP Fraud Forensics: Identity Spoofing** Erkennung und Blockierung gefälschter Absender-Identitäten.
atp-ff-fraud-attempt	**ATP Fraud Forensics: Fraud Attempt Analyses** Prüft die Authentizität und Integrität von Metadaten und Mailinhalten.
atp-ff-feign-facts	**ATP Fraud Forensics: Feign Facts Identification** Inhaltsanalyse von Nachrichten auf Basis von Vorspiegelung fingierter Tatsachen.
atp-freezing	**ATP E-Mail Freezing** „Einfrieren" der Mails bis zum erneuten Scan mit in Echtzeit aktualisierten Signaturen und Informationen zu Bedrohungslagen.
atp-mas	**ATP Massive Attack Prevention System** Kombination mehrerer Filterstufen zur Erkennung weitgefächerter globaler Angriffe

User: Empfänger der E-Mail

Date: Datum und Uhrzeit

Sender: From- und Envelope-Sender

Server Address: Die IP-Adresse des absendenden Mailservers

Attachment: Name des geblockten Anhangs

URL: Name der geblockten URL

Mit diesen Informationen ist der Kunde in der Lage, Angriffe näher zu analysieren und seine lokale IT-Infrastruktur entsprechend zu sichern.

2.8 Ex-Post-Alarmierung

In seltenen Fällen kann es vorkommen, dass eine bereits zugestellte E-Mail im Nachhinein als potentiell schädlich eingestuft werden muss. Dann wird automatisiert eine entsprechende Benachrichtigung an eine oder mehrere Kontaktpersonen aus dem Unternehmen des Kunden gesendet. Diese Benachrichtigung enthält Informationen zur Art der Attacke sowie zur E-Mail selbst, die zugestellt wurde. Mit den kommunizierten Informationen ist die Kontaktperson anschließend in der Lage, die Attacke zu rasch zu überprüfen, sodass die Gefahrenlage kurzfristig nach Eingang der potentiell schädlichen E-Mail eingedämmt werden kann.

2.9 ATP Report

Eine gute, detaillierte Auskunft über durchgeführte Analysen der E-Mail-Attachments gewährt der ATP-Report von Hornetsecurity. Dieser Report ist in vier Hauptfenster eingeteilt:

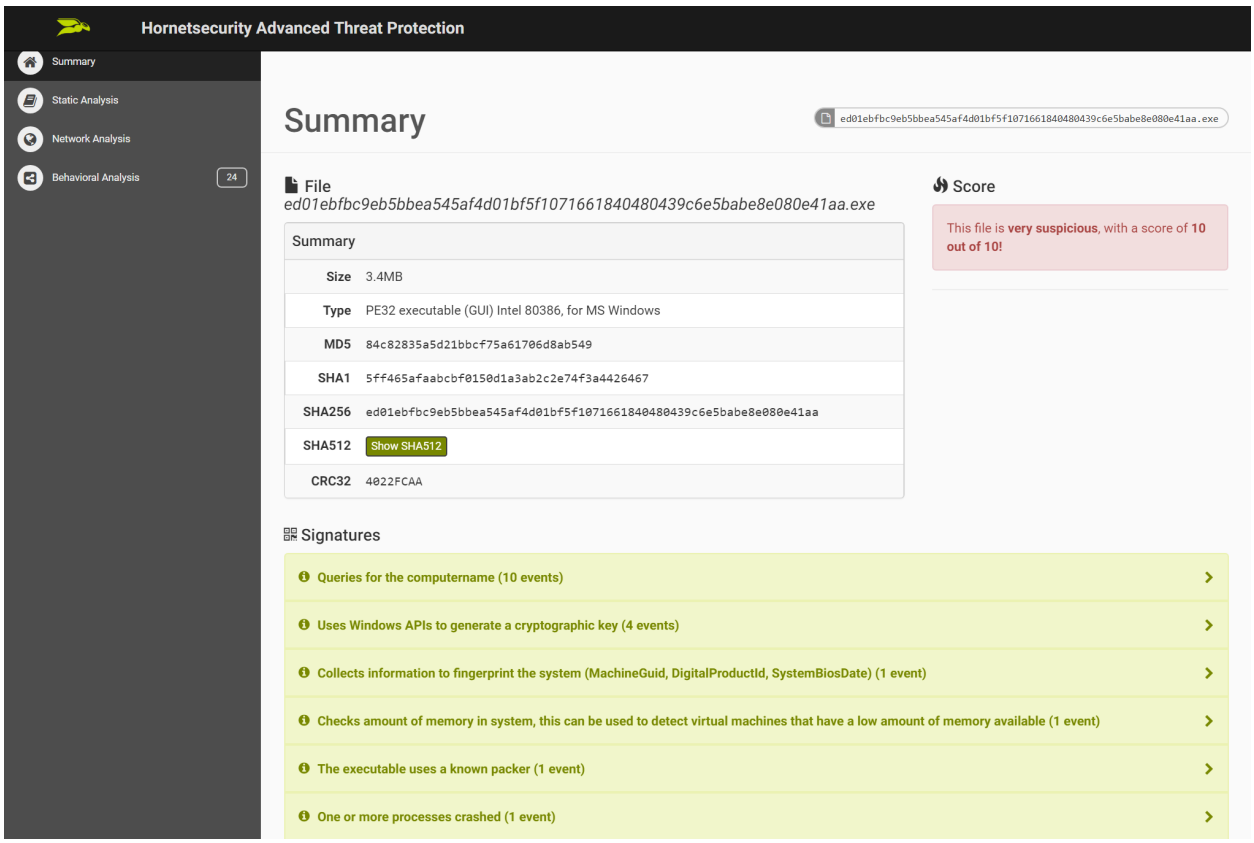

Abbildung 11: Beispiel eines ATP-Reports

- *Summary/Zusammenfassung:*

  Zunächst erhält der Betrachter des Reports einen Überblick über die analysierte Datei („File"). Des Weiteren liegt ihm eine Einschätzung der Gefährlichkeit vor: Der „Score" reicht dabei von 0 (ungefährlich) bis 10 (höchste Gefahrenstufe). Im Abschnitt „Signatures" wiederum ist das Verhalten des untersuchten Objekts in drei Kategorien eingeteilt: (Information, Achtung, Warnung). Mit Klick auf eine Signatur erhält der Leser weitere Prozessinformationen.

- *Static Analysis:*

  In diesem Abschnitt gibt es drei Unterkategorien:

  - Static Analysis: Hier befinden sich die Ergebnisse der statischen Dateianalyse.
  - Strings: Die vorkommenden Zeichenketten der Datei sind hier aufgelistet.
  - Antivirus: Alle eingesetzten Antiviren-Filter und deren Ergebnisse lassen sich hier nachlesen.

- *Network Analysis:*

  Die Netzwerkanalyse verschafft einen guten Überblick über den gesamten Netzwerkverkehr im Zusammenhang mit der untersuchten Datei. Dieser wird im Report nach Protokollen wie http, TCP oder UDP aufgelistet.

- *Behavioral Analysis:*

  Das untersuchte Verhalten der E-Mail-Anhänge findet hier seine Darstellung. Dazu werden alle System-API-Calls, aber auch Prozesse aus der Sandbox-Analyse (siehe Abschnitt „Sandbox-Engine") aufgeführt.

3 Weitere Leistungen und Services

3.1 Spamfilter

Grundlage für den Einsatz von Hornetsecurity ATP ist der Hornetsecurity Spamfilter Service. Dieser eliminiert garantierte 99,9 Prozent an Spam-E-Mails sowie 99,99 Prozent Viren-Mails und nimmt somit Last von den Erkennungsmechanismen von Hornetsecurity ATP.

Beim Spamfilter Service kommen mehrere Erkennungsstufen zum Einsatz (Abbildung 12): In der Vor-Analyse blockiert die Lösung bereits den Großteil aller eintreffenden Spamnachrichten ab, so dass diese erst gar nicht in die Aktive Analyse gelangen. Dort wiederum greift eine Vielzahl an Filtersystemen und Analyse-Engines ein und trennt die korrekten, gewollten E-Mails von verdächtigen Nachrichten. Letztere werden in die Quarantäne gelegt, wo sie der Postfachbesitzer per Spamreport oder über das Control Panel überprüfen und sie sich gegebenenfalls zustellen kann.

Zusätzlich bietet der Spamfilter Service unter anderem die folgenden Features:

- Infomail-Filter, um Newsletter oder andere werbliche E-Mails herauszufiltern
- Content-Filter, um Attachments zu untersuchen oder Anhänge von der eigentlichen E-Mail zu trennen.
- Erweitertes E-Mail-Routing zur Zuweisung von E-Mails auf verschiedene Mailserver
- Schutz vor DDoS-Angriffen

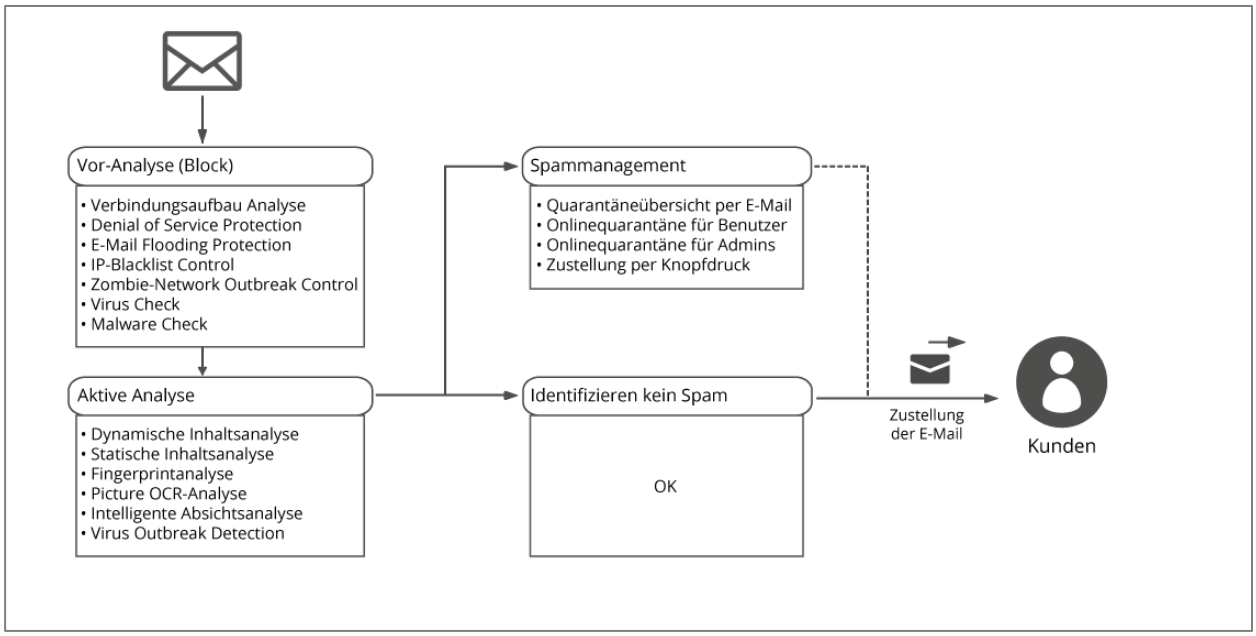

Abbildung 12: Schematischer Überblick über das Spammanagement von Hornetsecurity

3.2 E-Mail-Archivierung (Aeternum)

Im E-Mail-Archiv werden alle ein- und ausgehenden E-Mails für einen einstellbaren Zeitraum sicher archiviert, z. B. für 10 Jahre. Die Archivierung erfolgt parallel zur Auslieferung der E-Mail an den Empfänger, dadurch sind Manipulationen vor der Speicherung im Archiv ausgeschlossen. Das Hornetsecurity E-Mail-Archiv erfüllt damit die Anforderungen einer revisionssicheren Archivierung. Zur Aktivierung des Service genügt ein Knopfdruck im Control Panel.

Über die Anbindung an den Mailserver können auch intern verschickte E-Mails archiviert werden. Genutzt wird dazu die Journaling-Funktion des Mailservers, die alle E-Mails in einem Journal-Postfach bereitstellt, aus dem sie vom Hornetsecurity E-Mail Archive Service automatisch abgeholt werden. E-Mails im Archiv können über das Hornetsecurity Control Panel zugestellt werden. Über das Hornetsecurity Outlook Plugin ist ein direkter Zugriff auf im Archiv gespeicherte E-Mails möglich.

Wesentliche Features des E-Mail Archive Service:

- Automatische Archivierung ein- und ausgehender E-Mails, optional auch interner E-Mails
- Revisionssichere Ablage mit konfigurierbarer Speicherdauer; z. B. 10 Jahre
- Volltextindex mit indizierten Anhängen
- Outlook Plugin zur Suche, Weiterleitung und Nacharchivierung

Weitere Details zum E-Mail Archive Service entnehmen Sie bitte der Produktdokumentation.

3.3 E-Mail Verschlüsselung

E-Mails werden in der Regel unverschlüsselt durch das Internet übertragen. Grundsätzlich ist die Verschlüsselung des Transportwegs per TLS (Transport Layer Security) möglich, d. h. nicht die E-Mails selber, sondern der Übertragungskanal wird verschlüsselt. Hornetsecurity nutzt grundsätzlich TLS zur Übermittlung von E-Mails durch das Internet, sofern die Gegenseite ebenfalls TLS unterstützt. Damit sind E-Mails während der Übertragung von einem Mailserver auf den nächsten Mailserver vor Einblick und Veränderung durch Dritte geschützt.

Obwohl viele Mailserver bereits TLS unterstützen, hat sich dessen Benutzung allerdings bisher nicht vollständig durchsetzen können. Ein anderer und auch sichererer Ansatz, die Verschlüsselung der E-Mails selber (nicht des Transportwegs) zwischen Sender und Empfänger, z. B. per S/MIME, wird zwar von vielen Mailprogrammen unterstützt, ist aber sehr aufwändig in der Umsetzung und Betreuung.

Die Alternative ist der Verschlüsselungsservice von Hornetsecurity. E-Mails werden damit im Gateway bei Hornetsecurity vor der Übertragung über das Internet automatisch signiert und verschlüsselt. Sie sind dadurch auf dem gesamten Weg bis zum Empfänger gegen unbefugte Einsicht und Veränderung durch Dritte geschützt. Eingehende E-Mails werden automatisch im Hornetsecurity Gateway entschlüsselt und über TLS geschützt auf den Mailserver des Kunden zugestellt. Die gesamte Schlüsselverwaltung ist automatisiert, welche E-Mails verschlüsselt werden, kann per Policy vom Kunden im Control Panel voreingestellt werden.

Weitere Details zum E-Mail Verschlüsselungsservice entnehmen Sie bitte der Produktdokumentation.

3.4 E-Mail Continuity

Als Option zum Hornetsecurity Spamfilter Service ist die Aktivierung des E-Mail Continuity Service möglich. Durch den Continuity Service wird E-Mail hochverfügbar: Im Fall des Ausfalls der E-Mail Infrastruktur auf Kundenseite schaltet der Continuity Service auf einen bereitgestellten E-Mail Server von Hornetsecurity um.

Die Umschaltung kann automatisch oder auf Anforderung durch den Hornetsecurity Support erfolgen, selektiv pro Benutzer oder für die gesamte Domain. Benutzer können dadurch trotz Ausfalls ihres Servers weiterhin E-Mail senden und empfangen.

Zusätzlich werden bei gebuchtem Continuity-Service die letzten drei Monate des Mailverkehrs in einem rollierenden Backup gesichert und zum Abruf über das Control Panel oder das Hornetsecurity Outlook Plugin vorgehalten. Damit können einzelne E-Mails oder der gesamte Mailverkehr eines Zeitraums wiederhergestellt und z. B. die Lücke seit dem letzten Backup geschlossen werden.

Weitere Details zum E-Mail Continuity Service entnehmen Sie bitte der Produktdokumentation.

4 Quellen

- Kapitel 1.1: Abschaltung des Providers McColo: https://en.wikipedia.org/wiki/McColo
- Kapitel 1.2.1: Schäden durch CEO Fraud: https://www.ic3.gov/media/2016/160614.aspx
- Kapitel 1.4: BSI-Leitlinie zur Internet-Sicherheit "Sichere Nutzung von E-Mail (ISi-Mail-Client)" https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_mail_client_leitlinie_pdf.pdf?__blob=publicationFile (Version 1.0, Stand 22.03.2016)
- Kapitel 1.4: Zum Thema Ransomware - Bedrohungslage, Prävention & Reaktion: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html
- Kapitel 1.5: Beispiel Ransomware-Angriffs auf das Krankenhaus in Neuss: https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html
- Kapitel 1.5: Grafik des BSI zu den betrieblichen Auswirkungen einer Infektion mit Ransomware http://ap-verlag.de/clickandbuilds/WordPress/MyCMS4/wp-content/uploads/2016/09/grafik-bsi-auswirkungen-infektion-ransomware.jpg

Hornetsecurity ist Mitglied bei: