FireEye

FireEye Report

Die häufigsten Begriffe bei Spear-Phishing-Angriffen, mit denen Cyberkriminelle in Netzwerke eindringen und Daten stehlen

Inhalt

Zusammenfassung

Cyberkriminelle haben durch unzureichende Abwehrmaßnahmen und ahnungslose Anwender heute oft leichtes Spiel, Advanced Malware in Netzwerke einzuschleusen – Malware, die die Systeme von Organisationen attackiert und damit eine Vielzahl bösartiger Aktivitäten ermöglicht. Ein Großteil dieser Advanced Malware wird per E-Mail mit schädlichen Dateianhängen übertragen. Dieser Bericht untersucht die Dateien, die von Cyberkriminellen verbreitet werden – und hier vor allem die, die es schaffen, traditionelle Abwehrmaßnahmen wie z. B. Firewalls, Next Generation Firewalls, Intrusion-Prevention-Systeme (IPS), Antiviren-Programme (AV) und Secure Gateways zu umgehen. Er beschreibt die Begriffe, die in den für diese Advanced Malware charakteristischen Dateinamen und Dateitypen verwendet werden, und liefert Anwendern und Sicherheitsteams, die sich vor diesen Advanced Threats schützen wollen, wichtige Informationen.

Einführung

Trotz aller Abwehrmaßnahmen, die den E-Mail-Verkehr schützen sollen, bietet dieser Kanal Cyber-kriminellen nach wie vor zahlreiche Möglichkeiten. E-Mail ist das häufigst genutzte Medium bei Angriffen. Und die Risiken, die mit diesen Angriffen einhergehen, sind beträchtlich. Per E-Mail treffen jedoch nicht nur Spam und massenweise Advanced Malware ein. Auch viele Advanced-Persistent-Threat-Angriffe (APT) werden per E-Mail ausgelöst. GhostNet, Night Dragon, Operation Aurora, die RSA-Bruchstellen und viele andere öffentlich dokumentierte APT-Angriffe erfolgten zumindest teilweise über gezielte Spear-Phishing-E-Mails.

Cyberkriminelle halten an dieser Angriffsweise fest weil es so einfach funktioniert. Im neuesten Advanced-Threat-Bericht für das erste Halbjahr 2012 von FireEye, ist belegt, dass die Zahl bösartiger E-Mails zwischen dem ersten und zweiten Quartal 2012 um 56 Prozent gestiegen sei. Anzumerken ist, dass sich diese Zunahme nicht auf die Gesamtzahl aller verbreiteten bösartigen E-Mails bezieht, sondern auf die mengenmäßige Zunahme der E-Mails, mit denen Cyberkriminelle es geschafft haben, die bestehenden traditionellen Abwehrmaßnahmen von Organisationen zu umgehen.

Hunderte Kunden aus aller Welt nutzen derzeit das Malware Protection System™ (MPS) von FireEye. Diese Unternehmen sind damit in einer einzigartigen Position, sich gegen diese komplexen, Advanced Cyber-Threats zu schützen. Die Lösungen von FireEye werden hinter Firewalls, Next Generation Firewalls, Intrusion-Prevention-Systeme (IPS), Antiviren-Programmen und anderen Security-Gateways eingesetzt. Sie bilden damit die letzte Abwehrlinie für die anwendende Organisation. Die Appliances dieser Lösung sammeln automatisch Details über die einzelnen Bedrohungen, die daraufhin aggregiert, analysiert und weitergegeben werden können. Die Lösungen von FireEye ermöglichen einen detaillierten Report über die Eigenschaften von Advanced Threats.

Dieser Bericht fokussiert Eigenschaften von Advanced Malware, die über E-Mail-Anhänge verbreitet wird und traditionelle Abwehrmaßnahmen umgeht. Diese Daten liefern wichtige Einsichten in die Beschaffenheit von Advanced Malware und die Taktiken von Cyberkriminellen, sodass Sicherheits-teams und Anwender heutige Bedrohungen besser verstehen können. Hervorzuheben ist, dass sich die folgenden Informationen auf Advanced Threats beziehen, die bestehende Abwehrmaßnahmen umgehen können. Anders ausgedrückt, ist es sehr wahrscheinlich, dass diese Malware-Formen bald schon auch in Ihrem Postfach eintreffen werden – wenn Ihre Systeme nicht schon jetzt befallen sind.

Dateinamen

Cyberkriminelle verbreiten vorsätzlich Malware-Dateien damit diese von ahnungslosen Anwendern auf ihre lokalen Rechner heruntergeladen oder installiert werden. Dazu werden vielfältige Taktiken verwendet. Die verwendeten Wörter in den Dateinamen lassen dabei recht klare Rückschlüsse auf die Taktiken zu, auf welche die Cyberkriminellen im jeweiligen Fall setzen und die sich als „wirkungsvoll“ erwiesen haben. Die nachfolgende Tabelle zeigt die am häufigsten vorkommenden Wörter in Malware-Dateien, die von FireEye-Lösungen aufgespürt wurden. Es sind ganz klar diese Begriffe, mit denen Betrüger immer wieder traditionelle IT-Sicherheitsfunktionen umgehen.

2. Halbjahr 2011

Rang	Begriff	Anteil der Anhänge
1	label	15,17
2	invoice	13,81
3	post	11,27
4	document	10,92
5	postal	9,80
6	calculations	8,98
7	copy	8,93
8	fedex	6,94
9	statement	6,12
10	financial	6,12
11	dhl	5,20
12	usps	4,63
13	8	4,32
14	notification	4,27
15	n	4,22
16	irs	3,60
17	ups	3,46
18	no	2,84
19	delivery	2,61
20	ticket	2,60

1. Halbjahr 2012

Rang	Begriff	Anteil der Anhänge
1	dhl	23,42
2	notification	23,37
3	delivery	12,35
4	express	11,71
5	2012	11,30
6	label	11,16
7	shipment	9,88
8	ups	9,47
9	international	8,94
10	parcel	8,17
11	post	6,95
12	confirmation	5,81
13	alert	5,80
14	usps	5,80
15	report	5,79
16	jan2012	5,52
17	april	4,71
18	idnotification	3,60
19	ticket	3,58
20	shipping	2,92

Die obigen Tabellen zeigen die prozentualen Anteile der Begriffe die in bösartigen Anhängen verwendet und die von FireEye's MPS™-Systemen erkannt wurden. Hinweis: Da ein einzelner bösartiger Anhang mehrere Begriffe enthalten kann, ergeben die Anteile in Summe nicht 100 Prozent.

Eine Masche, mit der Cyberkriminelle Anwender hinters Licht führen, ist der Versand von Dateien, die den Anschein einer Benachrichtigung über eine Express-Lieferung erwecken. Durch die weite Verbreitung dieser Dienstleistungen und die mit ihnen assoziierte Wichtigkeit und Dringlichkeit denken Anwender oft nicht lange nach und öffnen die als Versandinformation getarnte Malware-Datei einfach. Tatsächlich ist diese Masche eine der häufigsten: 26 % aller Begriffe in Malware-Dateinamen sowie 7 der 10 häufigsten Begriffe im ersten Halbjahr 2012 entfallen auf den Versandbereich. Beispiele für diese Art Dateinamen der Cyberkriminellen sind „DHL document.zip“, „Fedex_Invoice.zip“ und „Label_Parcel_IS741-1345US.zip“.

Im Zeitraum vom zweiten Halbjahr 2011 bis zum ersten Halbjahr 2012 zeichneten sich verschiedene Trends ab. Zum Beispiel stieg der Anteil der Dateinamen mit versandbezogenen Wörtern von 19,20 auf 26,33 Prozent. Der Anteil der Dateien mit Wörtern, die eine Dringlichkeit vorgaben, kletterte von 1,72 auf 10,68 Prozent.

2. Halbjahr 2011

Thema	Anteil gesamt
Versand	19,20
Bank/Steuern	5,98
Dringlichkeit	1,72
Airline	1,81
Rechnung	4,98

1. Halbjahr 2012

Thema	Anteil gesamt
Versand	26,33
Bank/Steuern	3,83
Dringlichkeit	10,68
Airline	2,45
Rechnung	0,68

Die obigen Tabellen zeigen die fünf häufigsten in bösartigen E-Mail-Anhängen verwendeten Begriffskategorien.

Hier weitere häufig verwendete Kategorien:

- **Dringlichkeit.** Begriffe mit einem Bezug auf Dringlichkeit wie z. B. „Bestätigung“, „Warnung“ und „Benachrichtigung“ machen die zweithäufigste Kategorie aus. Die Begriffe können dabei für sich stehen, wurden aber auch oft in Verbindung mit anderen Kategorien beobachtet, u. a. mit Versand (z. B. „UPS-Delivery-Confirmation-Alert_April-2012_215759.zip“) oder Steuern (z. B. „IRS-Penalty-Income-Tax-Warning-Notification-28306SUD4811L9JS.zip“).
- **Finanzen.** Bezugnahmen auf Finanzinstitutionen und zugehörige Transaktionen und Mitteilungen waren ebenfalls oft zu beobachten. Dateinamen waren u. a. „VisaCard-N486102989.zip“, „PayPal.com_2012_Account_Update_Form.html“ und „Lloyds TSB - Login Form.html“.
- **Steuern.** Sehr häufig wurden auch Bezugnahmen auf Steuern und die US-Finanzbehörde IRS beobachtet, mit Dateinamen wie „Tax_Refund.zip“, „irspdf.zip“ und „tax_return_form.pif“.
- **Reisen.** Zahlreiche Dateinamen ließen auf Reisebuchungen und typischerweise hier Flug-reservierungen schließen, mit Bezeichnungen wie „Ticket_American_Airlines_ID3457-144.zip“, „Delta_Air_Lines_Ticket_ID271-3714.zip“ und „A_Airline_Ticket_ID279-44-357US.zip“.
- **Rechnungen.** Eine weitere große Kategorie bildeten Begriffe rund um Rechnungen, Aufträge usw., mit Dateinamen wie „Purchase Order 74457.zip“, „Invoice_ID757731.zip“ und „Invoice_Copy.zip“.

Die fünf häufigsten Dateiendungen

Bei den Endungen bzw. Erweiterungen von Malware-Dateien orientieren sich Cyberkriminelle an den Entwicklungen der Sicherheitsvorkehrungen und -mechanismen. Deutlich zu erkennen ist die Abkehr von EXE-Dateien. Diese früher mit Abstand häufigste Endung von Malware-Anhängen kommt heute kaum noch an den Sicherheitsfunktionen vorbei. EXE-Dateien lösen zudem oft Warnungen im Computer-Betriebssystem des Anwenders aus. Der Anwender wird aufgefordert, die Installation einer EXE-Datei zu bestätigen – was die Wahrscheinlichkeit, dass Malware das betreffende System infizieren kann, weiter verringert.

2. Halbjahr 2011

Jahr	Dateiendungen	Anteil
2011	zip	85,79
2011	exe	5,91
2011	pif	2,67
2011	scr	2,06
2011	bat	1,79

1. Halbjahr 2012

Jahr	Dateiendungen	Anteil
2012	zip	76,91
2012	pdf	11,79
2012	exe	3,98
2012	doc	2,67
2012	pif	1,09

Die obigen Tabellen zeigen die relativen Anteile der Dateiendungen von bösartigen Dateien, die von FireEye's MPS™-Systemen erkannt wurden.

Die überwältigende Mehrheit komplexer Malware-Dateien wird heute als Zip-Datei erstellt – stolze 76,91 Prozent. Die Komplexität dieser Anhänge, die oft vielfältige eigenständige Dateien und Dateitypen enthalten – verbunden mit dem mangelnden Bewußtsein der Anwender, wie gefährlich bestimmte Dateiendungen sein können – macht diesen Dateityp zu einem äußerst effektiven Instrument zur Verbreitung von Malware und Ausnutzen von System-Schwächen.

Auch PDF-Dateien stellen eine ernste Bedrohung dar. Auf diesen Dateityp trifft man überall; fast jeder Computeranwender kennt ihn. Dennoch wissen viele Anwender nicht, dass Malware auch über PDF-Dateien verbreitet werden kann. Zudem wird in PDF-Dateien eingebettete Malware von konventionellen Schutzprogrammen nur schwer erkannt. Das PDF-Format bietet Internetbetrügern damit ein sehr effektives Angriffsinstrument.

Fazit

Durch den Bezug auf wichtig und meist zeitsensibel erscheinende Informationen – Express-Lieferungen, Steuerbelege, den Kontostatus, Flugtickets usw. – erzeugen Cyberkriminelle bei Empfängern ein Gefühl von Dringlichkeit. Die Empfänger sollen veranlaßt werden, die Malware ohne Weiteres auf ihr System herunterzuladen. Da EXE-Dateien für Cyberkriminelle heute weniger „wirksam“ sind, setzen sie nun mehr auf Dateitypen wie ZIP, PDF und andere, um bestehende traditionelle Sicherheitsfunktionen zu umgehen. Um sich gegen diese Bedrohungen zu wappnen, müssen sich die Anwender daher nicht nur über die Gefahren durch Advanced Malware allgemein informieren, sondern auch über die vielfältigen Formen, in denen diese heute auftreten kann. Darüber hinaus sind die für Sicherheit zuständigen Teams heute auf Technologien angewiesen, die diese komplexen Bedrohungen, welche konventionelle Schutzfunktionen umgehen, tatsächlich erkennen und stoppen können. Anwender müssen sich zu ihrem eigenen Schutz über Spear-Fishing-E-Mails informieren – vor allem darüber, wie „authentisch“ diese aufgemacht sein können, und über die Gefahren, die diese Programme bergen. Um sich vor gezielten Advanced Threats zu schützen und diese zu blocken, vertrauen Unternehmen zunehmend auf Next Generation Sicherungslösungen – Lösungen, welche genau die Angriffe, die traditionelle Sicherheitslösungen nicht erkennen, abwehren können.

Über FireEye, Inc.

FireEye ist ein führendes Unternehmen bei der Abwehr von Advanced Maware, Zero-Day-Exploits und APT-Taktiken. Die Lösungen von FireEye ergänzen dabei traditionelle Abwehrsysteme wie Firewalls, Next-Generation Firewalls, IPS/IDS sowie Antiviren-Programme und Gateways, die komplexere Angriffe nicht stoppen können und so Sicherheitslücken im Netzwerk offen lassen. FireEye liefert branchenweit die einzige Lösung, die sowohl Angriffsvektoren über Web und E-Mail entdeckt und stoppt als auch latent versteckte Schadsoftware in Dateien findet. Sie deckt alle Phasen des Angriffszyklus ab – mit einer signaturlosen Engine, die eine zustandsorientierte Analyse des jeweiligen Angriffs vornimmt um Zero-Day-Bedrohungen erkennen zu können. FireEye ist in Milpitas, Kalifornien (USA) ansässig und wird von führenden Finanzpartnern unterstützt, darunter Sequoia Capital, Norwest Venture Partners und Juniper Networks.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035, USA | Tel.: +1-408-321-6300 | E-Mail: info@FireEye.com | Web: www.FireEye.com