



KASPERSKY^{LAB}

Kaspersky Security Bulletin:

JAHRESANALYSE FÜR 2018/2019

Vicente Diaz

INHALTSVERZEICHNIS

Keine großen APTs mehr	4
Netzwerkhardware und Internet der Dinge (IoT)	5
Öffentliche Vergeltungsmaßnahmen	6
Viele Newcomer	7
Negative Ringe.....	8
Der beliebteste Angriffsvektor	9
Verheerender Destroyer	10
Angriffsvektor Lieferkette	11
Der mobile Bereich	12
Weitere Aspekte.....	13

Nichts ist schwieriger als Vorhersagen. Anstatt also in die magische Kristallkugel zu blicken, möchte ich anhand vergangener Entwicklungen und aktueller Trends ermitteln, was uns in den kommenden Monaten erwarten könnte. Hierzu habe ich einige der intelligentesten Menschen befragt, die ich kenne, und konzentriere mich bei unserem Szenario auf APT-Angriffe, da diese erfahrungsgemäß die größte Innovation beim Umgehen von Sicherheitssystemen aufweisen. Im Folgenden finden Sie also unsere Prognosen für die nächsten Monate.

KEINE GROSSEN APTS MEHR

Wie bitte? Wie kann es sein, dass – obwohl wir scheinbar täglich neue Bedrohungen entdecken – die erste Vorhersage das genaue Gegenteil aussagt?

Grund hierfür ist, dass die Sicherheitsbranche immer wieder hochkomplexe, von Regierungen finanzierte Angriffe entdeckt hat, die Jahre der Vorbereitung erforderten. Die logische Konsequenz für Angreifer ist es, neue und sogar noch komplexere Techniken zu entwickeln, die noch schwieriger zu entdecken und ihren Urhebern noch schwerer zuzuordnen sind.

Und hierzu gibt es verschiedenste Möglichkeiten. Die einzige Anforderung ist ein Verständnis der von der Branche genutzten Methoden zur Bedrohungszuordnung sowie zur Erkennung von Gemeinsamkeiten der Attacken und der dafür verwendeten Artefakte – und diese sind scheinbar kein großes Geheimnis. Mit genügend Ressourcen kann eine einfache Lösung für einen Angreifer darin bestehen, verschiedene laufende Aktivitäten zu haben, die nur schwer demselben Ursprung oder derselben Bedrohung zuzuordnen sind. Gut ausgestattete Angreifer können neue innovative Methoden implementieren, während sie die alten weiter am Leben erhalten. Natürlich steigt die Chance, dass alte Bedrohungen entdeckt werden. Die neuen zu finden, ist jedoch eine weitaus größere Herausforderung. Anstatt immer raffiniertere Kampagnen zu entwickeln, ist es für manche Akteure mit den richtigen Mitteln anscheinend effizienter, direkt die Infrastrukturen und Unternehmen anzugreifen, in denen ihre eigentlichen Opfer zu finden sind. Hierzu zählen beispielsweise Internetanbieter. Manchmal lässt sich dies durch Regulierung erreichen, ohne dass Malware erforderlich ist.

Manche Vorgänge werden einfach an verschiedene Gruppen und Unternehmen outgesourct, die unterschiedliche Tools und Techniken einsetzen. Hierdurch gestaltet sich die Zuordnung äußerst schwierig. Bei Angriffen, die von Regierungen finanziert werden, kann sich diese Art der Verteilung von Ressourcen und Talenten auf die künftige Entwicklung entsprechender Kampagnen auswirken. Technologien und Tools stammen in diesem Szenario aus dem privaten Sektor und stehen für jeden Kunden zum Kauf bereit, ohne dass dieser die technischen Details oder Konsequenzen kennen muss.

All das zeigt, dass wir wahrscheinlich kaum noch große und komplexe Angriffe entdecken, sondern dass Angreifer auf neue Methoden setzen werden.

NETZWERKHARDWARE UND INTERNET DER DINGE (IOT)

Fast jeder Angreifer hat schon einmal Methoden und Tools eingesetzt, die darauf abzielen, Netzwerkhardware anzugreifen. Kampagnen wie VPNFilter sind ein gutes Beispiel dafür, dass Angreifer seit einiger Zeit schon ihre Malware zum Aufbau vielseitiger Botnets einsetzen. In diesem speziellen Fall dauerte es lange, bis der Angriff erkannt wurde – obwohl die Malware so weit verbreitet war. Das ist äußerst besorgniserregend, wenn man die Folgen für gezieltere Angriffe bedenkt.

Doch die Idee geht bei gut ausgestatteten Cyberkriminellen noch weiter: Warum sich auf das Zielunternehmen konzentrieren, wenn man auch direkt die zugrunde liegende Infrastruktur angreifen kann? Soweit wir wissen, waren entsprechende Versuche bisher noch nicht erfolgreich, doch die bisherigen Beispiele wie Regin zeigen, wie verlockend ein solches Maß an Kontrolle für Angreifer ist.

Schwachstellen in Netzwerkhardware ermöglichen Cyberkriminellen unterschiedliche Angriffsvektoren. Sie können mit umfangreichen Infektionen Botnets aufbauen, die sie später für unterschiedliche Ziele einsetzen, oder sie zielen mit unauffälligeren Angriffen auf ausgewählte Ziele ab. In dieser zweiten Gruppe müssen wir auch „malwarelose“ Angriffe berücksichtigen, bei denen schon das bloße Öffnen eines VPN-Tunnels zum Spiegeln oder Umleiten des Datenverkehrs Angreifern die erforderlichen Informationen bieten kann.

Alle diese Netzwerkelemente können auch Teil des riesigen Internet of Things (IoT) sein, in dem Botnets scheinbar unaufhaltsam wachsen. Diese Botnets können in den falschen Händen unglaublich leistungsfähig sein, wenn es beispielsweise darum geht, kritische Infrastrukturen zu stören. Und Cyberkriminelle mit den richtigen Mitteln könnten diese Leistung sogar für terroristische Angriffe nutzen. Ein Beispiel für die Vielseitigkeit von Botnets sind Frequenzsprungverfahren: Hierdurch umgehen die Bedrohungen Überwachungstools, indem sie die herkömmlichen Exfiltrationskanäle meiden.

Obwohl jedes Jahr erneut vor Botnets gewarnt wird, dürfen wir IoT-Botnets nicht unterschätzen – denn sie werden immer stärker.

ÖFFENTLICHE VERGELTUNGSMASSNAHMEN

Eine der größten Fragen in Sachen Diplomatie und Geopolitik beschäftigt sich mit dem Umgang mit aktiven Cyberangriffen. Die Antwort ist nicht einfach und hängt neben anderen Aspekten davon ab, wie schwer und offensichtlich der Angriff ist. Nach Angriffen wie dem auf das Democratic National Committee (DNC) hat sich die Lage jedoch scheinbar verschärft.

Nach Untersuchungen kürzlicher Angriffe mit hoher medialer Aufmerksamkeit, wie z. B. den Hacks des Sony Entertainment Network oder auch der angesprochenen Attacke auf das DNC, wurde eine ganze Liste von Verdächtigen angeklagt. Dies bedeutet für die entsprechenden Personen nicht nur Gerichtsverfahren, sondern auch eine öffentliche Zurschaustellung der vermeintlichen Urheber des Angriffs. Diese lässt sich wiederum nutzen, um im Rahmen einer Diskussion um schwerwiegendere diplomatische Folgen Meinungen zu beeinflussen.

Tatsächlich haben wir in der Vergangenheit erlebt, wie Russland aufgrund vermeintlicher Eingriffe in demokratische Prozesse solche Folgen zu spüren bekam. Hierdurch denken andere vielleicht zweimal nach, bevor sie entsprechende Aktionen starten.

Die Angst davor, dass so etwas passiert, oder der Gedanke, dass es bereits passiert sein könnte, ist jedoch der größte Erfolg der Angreifer. Denn jetzt können sie diese Angst, Unsicherheit und Zweifel auf verschiedene und subtilere Weise ausnutzen – wie es bei einigen Angriffen, wie denen der Shadowbrokers, bereits der Fall war. Und diese Fälle werden künftig weiter zunehmen.

Was werden wir in Zukunft also erleben? Diese Art der Propaganda wurde wahrscheinlich mit den vergangenen Angriffen nur ausgetestet. Wir glauben, dass dies erst der Anfang ist, uns hier künftig noch einiges erwartet und dass diese Methode auf verschiedenste Weise eingesetzt werden wird: beispielsweise in False-Flag-Angriffen, also Attacken unter „falscher Flagge“, wie Olympic Destroyer, für die der mögliche Ablauf und das eigentliche Ziel bis heute ungeklärt sind.

VIELE NEWCOMER

Einfach ausgedrückt lässt sich die Welt der APTs in zwei Gruppen aufteilen: klassische, gut ausgestattete und weit fortgeschrittene Akteure (die wahrscheinlich mit der Zeit verschwinden werden) und eine Gruppe motivierter Newcomer, die sich ebenfalls ein Stück vom Kuchen holen wollen.

Die Einstiegshürde war noch nie niedriger: interessierten Kriminellen stehen Hunderte effektive Tools, neu entwickelte geleakte Exploits und alle erdenklichen Frameworks zur Verfügung. Ein weiterer Vorteil für Kriminelle ist, dass diese Tools die Zuordnung von Bedrohungen nahezu unmöglich machen und sich bei Bedarf leicht anpassen lassen.

Es gibt zwei Regionen auf der Welt, in denen sich solche Gruppen zusehends verbreiten: Südostasien und der Nahe Osten. Wir haben die schnelle Entwicklung von Gruppen verfolgt, bei denen vermutet wird, dass sie sich in den entsprechenden Regionen befinden. Diese setzen in der Regel für lokale Ziele auf Social Engineering und nutzen schlecht geschützte Opfer sowie die fehlende Sicherheitskultur aus. Je mehr die Ziele jedoch ihre Verteidigung verbessern, desto mehr entwickeln auch die Angreifer ihre offensiven Fähigkeiten. So können sie mit zunehmenden technischen Möglichkeiten ihre Angriffe auch auf andere Regionen ausweiten. In diesem Szenario skriptbasierter Tools finden sich auch junge Unternehmen, die regionale Services anbieten und ihren Betrieb trotz OPSEC-Fehlschlägen weiter verbessern.

Ein interessanter technischer Aspekt ist die Tatsache, dass JavaScript-basierte Tools nach dem Exploit kurzfristig neu aufleben. Dies liegt an der nur schwierigen Beschränkung der Funktionalität durch Administratoren (im Gegensatz zu PowerShell), den fehlenden Systemprotokollen und der Möglichkeit, auch auf älteren Systemen ausgeführt zu werden.

NEGATIVE RINGE

Nach dem Jahr von Meltdown, Specter, AMDFlaws und all den zugehörigen Schwachstellen stellten wir uns folgende Frage: Wo findet sich die gefährlichste Malware? Und obwohl wir bisher kaum Bedrohungen entdeckt haben, die Schwachstellen unterhalb Ring 0 ausnutzen, ist schon die bloße Vorstellung erschreckend. Denn solche Angriffe wären für nahezu alle aktuellen Sicherheitsmechanismen unsichtbar.

Im Falle von SMM gab es seit 2015 mindestens einen öffentlich verfügbaren PoC (Point of Compromise). SMM ist eine CPU-Funktion, die sogar ohne Ring-0-Prozesse vollständigen Remotezugriff auf einen Computer bieten kann, einschließlich Zugriff auf den Arbeitsspeicher. Hier stellt sich natürlich die Frage, ob entsprechende Malware bisher nur nicht gefunden wurde, weil sie so schwer zu entdecken ist. Denn diese Funktion bietet einfach zu viele Möglichkeiten, als dass Cyberkriminelle sie ignorieren. Deshalb sind wir uns sicher, dass verschiedene Gruppen schon seit Jahren versuchen, entsprechende Mechanismen auszunutzen – vielleicht sogar erfolgreich.

Ähnliches erleben wir bei Virtualisierungs-/Hypervisor- bzw. bei UEFI-Malware. Bei beiden haben wir PoCs gefunden und HackingTeam hat sogar das UEFI-Persistenzmodul veröffentlicht, das seit mindestens 2014 verfügbar war. Doch auch hier sind in der Praxis keine Fälle aufgetreten.

Werden wir also jemals eines dieser seltenen Exemplare finden? Oder wurde diese Schwachstelle einfach noch nicht ausgenutzt? Letzteres scheint eher unwahrscheinlich.

DER BELIEBTESTE ANGRIFFSVEKTOR

Die wahrscheinlich am wenigsten überraschende Vorhersage dieses Artikels dreht sich um Spear-Phishing. Wir glauben, dass der bisher erfolgreichste Angriffsvektor in naher Zukunft sogar noch an Bedeutung gewinnen wird. Der Schlüssel zum Erfolg dieser Methode ist die Fähigkeit, das Opfer neugierig zu machen. Und dank kürzlicher riesiger Datenlecks bei verschiedenen Social-Media-Plattformen können Angreifer diese Methode weiter verbessern.

Die Daten aus Angriffen auf Social-Media-Giganten wie Facebook, Instagram, LinkedIn und Twitter stehen heute für jeden auf dem Schwarzmarkt zur Verfügung. In manchen Fällen ist es weiterhin unklar, welche Daten genau die Angreifer gestohlen haben. Sie können jedoch private Nachrichten und sogar Anmeldedaten umfassen. Für Social-Engineering-Angreifer sind diese Daten eine wahre Goldgrube. So nutzen manche Cyberkriminelle die gestohlenen Anmeldedaten aus, um unter dem Namen ihres Opfers einen engen Kontakt auf einer Social-Media-Plattform anzuschreiben. Hierbei erwähnen sie Privates aus vergangenen Nachrichten, um die Erfolgchancen eines Phishing-Angriffs deutlich zu erhöhen.

Dieser Ansatz lässt sich auch mit klassischen Scouting-Technologien kombinieren, bei denen Angreifer ihr Ziel mehrfach überprüfen, um sicherzustellen, dass es sich um das richtige Opfer handelt, und so die Verteilung (und Erkennung) von Malware minimieren. Bei Dateianhängen stellen die meisten Angreifer vor Auslösen schädlicher Aktivitäten sicher, dass eine menschliche Interaktion vorliegt, um automatische Erkennungssysteme zu umgehen.

Tatsächlich gibt es verschiedene Initiativen, die maschinelles Lernen einsetzen, um die Effektivität von Phishing zu optimieren. Es ist zwar nach wie vor unklar, welche Folgen dieser Ansatz in der Praxis hätte, jedoch wird deutlich, dass Spear-Phishing durch die Kombination dieser Faktoren auch in den kommenden Monaten einen äußerst effektiven Infektionsvektor darstellen wird – insbesondere über Social Media.

VERHEERENDER DESTROYER

Olympic Destroyer war einer der berüchtigtsten Fälle potenziell verheerender Malware des letzten Jahres. Doch viele Angreifer implementieren regelmäßig entsprechende Funktionen in ihre Kampagnen. Solche Angriffe, die große Schäden anrichten, bieten Angreifern viele Vorteile, insbesondere um Ablenkungen zu schaffen und nach dem Angriff Protokolle oder Beweise verschwinden zu lassen. Manchmal dienen sie auch einfach als fiese Überraschung für das Opfer.

Manche dieser Angriffe haben geostrategische Ziele, die aktuelle Konflikte betreffen, wie wir es in der Ukraine erlebt haben, oder verfolgen politische Interessen wie bei den Attacken auf verschiedene Ölfirmen in Saudi-Arabien. In manchen anderen Fällen sind sie auch das Ergebnis von Hacking oder die Aktivitäten einer vom eigentlichen Angreifer beauftragten Gruppe, da dieser unentdeckt bleiben möchte. Die Gemeinsamkeit all dieser Attacken ist, dass sie für Angreifer einfach zu gut sind, um nicht eingesetzt zu werden. Regierungen können diese Angriffe als Gegenschlag einsetzen, der irgendwo zwischen diplomatischer Reaktion und Kriegsakt liegt. Und manche Regierungen experimentieren tatsächlich in diese Richtung. Die meisten Angriffe werden vorab geplant. Dies umfasst die anfängliche Auskundschaftung des Opfers und das eigentliche Eindringen. Wir wissen nicht, bei wie vielen Opfern bereits alles für einen Angriff vorbereitet ist oder welches Arsenal die Angreifer für die Attacke auffahren.

ICS-Umgebungen und kritische Infrastrukturen sind für solche Angriffe besonders anfällig und obwohl Branche und Regierungen in den letzten Jahren viel Arbeit in die Verbesserung dieser Situation investiert haben, haben wir noch lange keinen Idealzustand erreicht. Deshalb glauben wir, dass wir – obwohl solche Attacken nie wirklich weit verbreitet sind – im nächsten Jahr einige erleben werden, insbesondere bei Gegenschlägen auf geopolitische Entscheidungen.

ANGRIFFSVEKTOR LIEFERKETTE

Dies ist einer der gefährlichsten Angriffsvektoren, der in den letzten zwei Jahren erfolgreich ausgenutzt wurde. Durch ihn hat fast jeder Nutzer schon einmal überlegt, wie viele Anbieter er eigentlich hat und wie sicher diese sind. Es gibt leider keine einfache Antwort auf diese Art von Angriffen.

Obwohl sich dieser Vektor perfekt für Angriffe auf ganze Branchen (ähnlich wie bei Watering-Hole-Angriffen) oder sogar ganze Länder eignet (wie bei NotPetya), ist er für gezieltere Angriffe nicht optimal, da das Erkennungsrisiko höher ist. Darüber hinaus haben wir auch willkürlichere Angriffe erlebt, wie z. B. die Injektion schädlichen Codes in öffentliche Repositories für allgemeine Bibliotheken. Letztere Methode kann in sorgfältig zeitlich gesteuerten Angriffen eingesetzt werden, wenn diese Bibliotheken in einem bestimmten Projekt verwendet werden – mit anschließender Entfernung des schädlichen Codes aus dem Repository.

Lässt sich diese Art von Angriff also auf gezieltere Weise einsetzen? Bei Software scheint dies schwieriger, da überall Spuren hinterlassen würden und die Malware wahrscheinlich an verschiedene Kunden verteilt würde. Realistischer ist der Einsatz in Fällen, in denen der Anbieter exklusiv für einen bestimmten Kunden arbeitet. Wie sieht es mit Hardware-Implantaten aus? Stellen sie eine realistische Möglichkeit dar? Dieses Thema wurde in letzter Zeit kontrovers diskutiert. Obwohl wir an Snowdens Leaks gesehen haben, wie sich Hardware auf dem Weg zum Kunden manipulieren lässt, scheint diese Methode nur für sehr einflussreiche Akteure möglich zu sein. Und selbst diese unterliegen hierbei diversen Einschränkungen. In Fällen, in denen der Käufer einer bestimmten Bestellung bekannt ist, ist es für den Angreifer meist einfacher, die Hardware am Ursprung anstatt auf dem Weg zum Kunden zu manipulieren.

Es ist nur schwer vorstellbar, dass alle technischen Kontrollen in der Herstellungskette umgangen werden können, um eine solche Manipulation durchzuführen. Wir wollen die Möglichkeit nicht ausschließen, aber hierzu wäre wahrscheinlich die Mitarbeit des Herstellers erforderlich.

Insgesamt stellen Angriffe auf die Lieferkette einen effektiven Infektionsvektor dar, von dem wir in Zukunft wahrscheinlich mehr hören werden. Hardware-Implantate halten wir jedoch für äußerst unwahrscheinlich. Und sollten sie doch einmal auftreten, werden wir es wohl nie erfahren.

DER MOBILE BEREICH

Mobilgeräte finden sich schon seit Jahren in solchen Prognosen. Hier erwarten wir zwar keine bahnbrechenden Veränderungen, jedoch sind in diesem Bereich die beiden unterschiedlichen Geschwindigkeiten interessant, die diese langsame Infektionswelle mit sich bringt. Wir müssen nicht erwähnen, dass alle Akteure Mobile-Komponenten in ihre Kampagnen implementieren. Warum sollten sie auch nur auf PCs abzielen? Tatsächlich gibt es viele Beispiele für Android-Artefakte, aber auch einige Verbesserungen bei Angriffen auf iOS.

Obwohl erfolgreiche Infektionen bei iPhones den Einsatz mehrerer Zero-Day-Schwachstellen erfordern, sollten man stets daran denken, dass Angreifer mit ausreichend Ressourcen entsprechende Technologien einkaufen können, um sie in kritischen Angriffen einzusetzen. Manche private Unternehmen behaupten, auf jedes iPhone zugreifen zu können, das ihnen physisch vorliegt. Andere, weniger gut ausgestattete Gruppen finden kreative Möglichkeiten, die Sicherheit dieser Geräte zu umgehen, z. B. mit MDM-Servern (Mobile Device Management), die Opfer nach erfolgreichem Social Engineering auf ihren Geräten ausführen und über die Angreifer schädliche Apps installieren können.

Hier ist es interessant, ob Angreifer durch den iOS-Bootcode, der Anfang des Jahres geleakt wurde, Vorteile erhalten oder ob sie neue Möglichkeiten finden, ihn auszunutzen.

So oder so erwarten wir in den kommenden Monaten zwar keinen großen Ausbruch zielgerichteter Malware für Mobilgeräte, aber anhaltende Aktivitäten durch fortschrittliche Angreifer, die versuchen, Zugang zu den Geräten ihrer Opfer zu erhalten.

WEITERE ASPEKTE

Welche Ideen haben Angreifer für die Zukunft? Eine der Ideen – insbesondere im Militärbereich – ist es, nicht länger auf fehleranfällige menschliche Interaktion, sondern auf mechanische Alternativen zu setzen. Angesichts dieser Tatsache und der vermeintlichen GRU-Agenten, die letzten April aus den Niederlanden ausgewiesen wurden, nachdem sie beispielsweise versucht hatten, sich in das WLAN-Netzwerk der OPCW zu hacken: Wie realistisch sind Drohnen, die anstelle menschlicher Agenten Hacks auf kurze Distanz übernehmen?

Und wie sieht es mit Backdoors in Kryptowährungen aus, über die Informationen oder sogar Geld gestohlen werden können?

Oder mit der Verwendung digitaler Waren für die Geldwäsche? Wie verhält es sich mit In-Game-Käufen und dem anschließenden Verkauf entsprechender Konten? Es gibt so viele verschiedene Möglichkeiten, dass die Prognosen der tatsächlichen Entwicklung selten gerecht werden. Die Komplexität des ganzen Umfelds ist nicht mehr vollständig überschaubar, sodass in verschiedenen Bereichen die Möglichkeiten für spezielle Angriffe steigen. Wie kann beispielsweise das interne Banking-System der Börse für Betrug missbraucht werden? Ich weiß es nicht. Ich weiß nicht einmal, ob ein solches System überhaupt existiert. Es ist nur ein Beispiel dafür, wie viele Möglichkeiten sich der Fantasie der Angreifer hinter diesen Kampagnen auftun.

Deshalb sind wir hier. Wir versuchen, die Angriffe zu antizipieren, die wir noch nicht verstehen und zu verhindern, dass sie in Zukunft auftreten.