Olivia von Westernhagen

Einbruch mit Komfort

Exploit-Kits als Basis moderner Cyber-Crime

Software as a Service – wochen- oder monatsweise zu mieten, mit einer Web-Oberfläche, die auch Computer-Laien bedienen können, professioneller Support inklusive. Nein, hier ist nicht von Microsofts oder IBMs neuestem Cloud-Angebot die Rede, sondern von der Infrastruktur krimineller Cyber-Gangs.

Montag, 18:15 Uhr. Wie jeden Abend schaut Gerald S. in sein E-Mail-Postfach; der Betreff „Letzte Mahnung“ fängt seine Aufmerksamkeit. Vermutlich, so denkt er, handelt es sich um Spam. Aber was, wenn ich doch eine Zahlungsfrist übersehen habe? In der E-Mail steht außer einem Link zur Rechnung auch das vollständige Impressum eines bekannten Elektronikversands, bei dem Gerald tatsächlich schon bestellt hat. Zwar ist ihm etwas mulmig, aber das Risiko eines Inkasso-Verfahrens will er nicht eingehen. Etwas unsicher klickt er auf den Link.

Es passiert – nichts: „Diese Seite existiert nicht“. Vielleicht, überlegt er, ist der Link zur Rechnung einfach fehlerhaft. Er nimmt sich vor, gleich am nächsten Tag beim Elektronikversand anzurufen, um den Sachverhalt zu klären. An dieser Stelle könnte diese banal anmutende Geschichte enden. Doch weit gefehlt: Als Gerald S. sich nämlich einige Minuten später Fotos vom letzten Ausflug mit seinen Freunden ansehen will, stellt er fest, dass sich diese nicht mehr öffnen lassen.

Digitale Erpresser

Eine Textdatei mit dem Titel DECRYPT_INSTRUCTION.txt klärt ihn darüber auf, dass seine Daten mit dem Kryptoverfahren RSA-2048 verschlüsselt wurden. Um Anweisungen zur Entschlüsselung zu erhalten, soll er den Anonymisierungsdienst Tor installieren und anschließend eine bestimmte Webseite besuchen. Gerald ist mit diesen Instruktionen restlos überfordert, versteht jedoch, dass die Erpresser den einzigen Schlüssel zu seinen Dateien besitzen. Prompt fällt ihm der Rechnungs-Link aus der E-Mail ein – aber auf der besuchten Seite war doch „nichts“ – oder?

Gerald ahnt nicht, dass der Quelltext der Seite verschlüsseltes JavaScript enthielt, welches sein Browser im Hintergrund ausgeführt hat. Das Skript analysierte systematisch sein System: Betriebssystem, Browser, installierte Plug-ins – einschließlich der jeweiligen Versionsnummern. Dabei fand es heraus, dass das Flash-Plug-in eine bekannte Sicherheitslücke enthielt, die es ausnutzen konnte.

Darüber lud das Skript dann die Erpresser-Software CryptoWall herunter und startete sie. Das Ganze geschah unbemerkt von der Antiviren-Software auf dem PC; Gerald hatte schon verloren, als er auf den Link geklickt hatte. Würde er die Anweisungen in der Text-Datei befolgen, so stünde er auf der aufzurufenden Webseite vor der Wahl, für die Entschlüsselung seiner Dateien eine vierstellige Summe zu bezahlen oder künftig auf seine Daten zu verzichten.

Hightech für Dummies

Beim Betrachten des Angriffsszenarios liegt die Vermutung nahe, dass es sich beim Angreifer um einen erfahrenen Cyberkriminellen handelt, der sowohl mit den technischen Details der angewandten Exploit-Technik vertraut ist als auch in der Lage sein muss, Malware zu programmieren. Keine der beiden Annahmen trifft zu.

Dank der seit einigen Jahren immer weiter um sich greifenden Exploit-Kits ist kein tiefgehendes Wissen mehr vonnöten, um Sicherheitslücken auf dem System des Angegriffenen aufzuspüren und darüber Schad-Code einzuschleusen. Steve Santorelli, Threat Researcher im Team Cymru Research NFP, definiert den Begriff Exploit-Kit so:

„Ein Komplettpaket, das alles enthält, um Systeme zu infizieren und diese auszunutzen, ohne dass man dazu sonderlich viel Programmierkenntnis benötigt – wenn überhaupt welche.“

Der letzte Teil dieser Aussage ist der Hauptgrund für die Beliebtheit dieses Angriffswerkzeugs – die Tatsache nämlich, dass zur Verwendung eines Exploit-Kits kaum technisches Wissen und erst recht keine Programmierkenntnisse notwendig sind.

Moderne Exploit-Kits verfügen über ein Web-Frontend, über das sich der Nutzer einloggen kann. Die grafische Oberfläche stellt Werkzeuge bereit, die das effektive automatisierte Verteilen der durch den Nutzer definierten Schadfunktion ermöglichen. Zu diesen Werkzeugen gehören neben den Exploits selbst unter anderem technischer Support, regelmäßige Updates und detaillierte Statistiken zu den gestarteten Malware-Kampagnen.

Zentraler Bestandteil eines Kits sind die Exploits. Dieser Code nutzt ganz gezielt eine Sicherheitslücke eines Programms aus; in der Regel lädt er heimlich im Hintergrund ein Schadprogramm aus dem Netz und führt es aus. Das Standard-Repertoire der Kits besteht aus Exploits für Sicherheitslücken in Java, Flash, Internet Explorer und Silverlight. Der Exploit-Kit-Nutzer bekommt detaillierte Statistiken, unter anderem zur Erfolgsquote der ihm zur Verfügung stehenden Exploits. Werte wie „Mehr als zehn Prozent aller Besucher erfolgreich infiziert“ sind keine Seltenheit. Gute Exploit-Kits garantieren ihren Nutzern Quoten von bis zu 20 Prozent.

Updates erweitern das Exploit-Repertoire regelmäßig. Werden neue Sicherheitslücken bekannt, liefern sich die Entwickler der Top-Produkte ein wahres Kopf-an-Kopf-Rennen: Schließlich ist es die beste Werbung, wenn man seinen Kunden als Erster funktionsfähige Exploits zur Verfügung stellen kann.

Die Königsdisziplin sind dabei sogenannte Zero-Day-Exploits, für die der Hersteller der betroffenen Software noch kein Update parat hat, das die Lücke stopft. Erst kürzlich förderte ein Datenleck bei Hacking Team, einem Hersteller von Überwachungs-Software, mehrere solcher Zero-Days zutage. Es dauerte nur Stunden, bis die Entwickler von Angler, Neutrino & Co. die Exploits bei sich eingebaut hatten und deren Kunden damit auf die Jagd nach neuen Opfern gehen konnten.

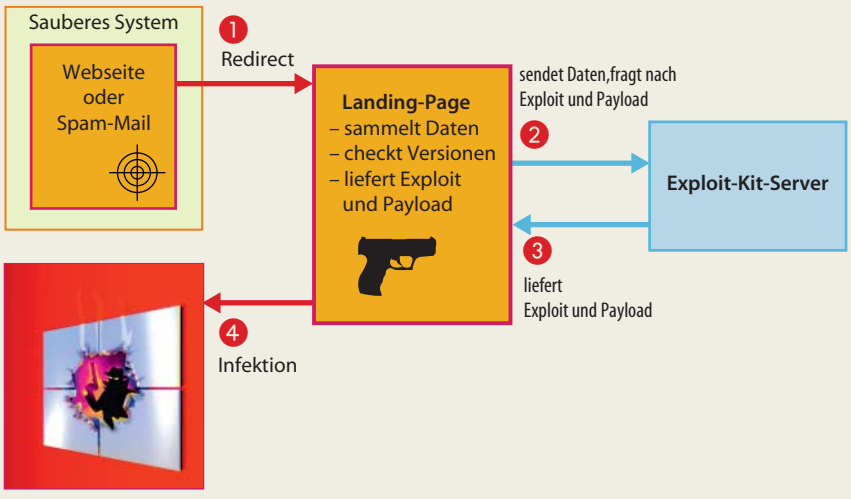
Geschäftsmodelle

Der Exploit erledigt nur den eigentlichen Angriff. Seine Aufgabe ist es, die sogenannte Payload auf dem Zielsystem zu installieren. Sie gehört typischerweise nicht zum Exploit-Kit; dessen Nutzer kann sie jedoch komforta-

Die Waffen der Hacker

Ablauf einer Infektion

Das Opfer öffnet eine Webseite und landet über einen Redirect auf der Landing-Page eines Exploit-Kits. Das Resultat: Das System des Opfers ist mit Schad-Software infiziert.



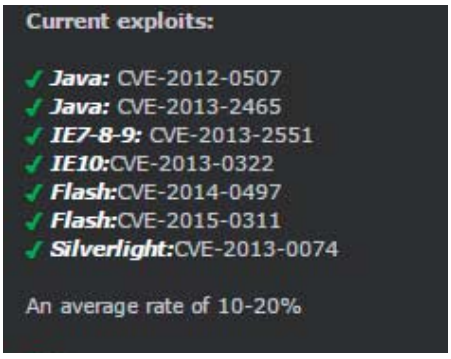
Die Werbebanner zeigen schon: Anders als VirusTotal sucht und findet dieser Scan-Service seine Kunden vor allem im kriminellen Umfeld.

bel über das Web-Interface hochladen und dann in seine aktuellen Kampagnen einbinden. Diverse Crimeware-Kits stellen passende Payloads so bereit, dass auch Laien sie mit wenigen Mausklicks „zusammenbasteln" können. Die Kombination eines Exploit-Kits mit weiterer kommerzieller Crimeware bietet somit ein Komplettpaket für Internetkriminelle, die ohne technisches Vorwissen schnelles Geld verdienen wollen.

Sehr beliebt ist derzeit Ransomware wie das eingangs beschriebene CryptoWall oder auch CryptoLocker, da sich damit ohne großen Aufwand viel Geld verdienen lässt. Offenbar ist ein beträchtlicher Teil der Opfer bereit, für den Zugang zu ihren verschlüsselten Daten zu zahlen. Die dreistelligen Beträge für die Nutzung eines Exploit-Kits für einige Wochen amortisieren sich schon mit wenigen zahlenden Opfern.

Ein Klassiker ist Schad-Software, die dafür sorgt, dass sich der infizierte Rechner einem Botnet anschließt. Ein auf diese Weise erstelltes Botnetz kann man dann etwa vermieten, um Spam zu versenden oder DDoS-Attacken auszuführen. Auch die bezahlte Installation weiterer Software – etwa Browser-Plug-ins für Klickbetrug oder die zwangsweise Anzeige von Werbe-Popups – ist ein lukratives Geschäftsmodell.

Exploit-Kits verteilen auch Schadprogramme für Online-Banking-Betrug und den allgemeinen Diebstahl von Zugangsdaten. Das ist



Der Reseller 0x43 bewirbt im Untergrundforum hackforums.net das RIG-Exploit-Kit.

dann aber schon eher etwas für Banden mit guten Verbindungen zum organisierten Verbrechen. Schließlich ist es mit einer gefälschten Überweisung nicht getan; das Geld muss weitergeleitet und gewaschen werden. Man braucht dazu unter anderem Money Mules in den jeweiligen Ländern, die ihr Konto als Überweisungsziel zur Verfügung stellen und das Geld gegen eine Provision etwa via Western Union weiterleiten.

Ein aktueller Trend bei den Payloads ist die dateilose Infektion, wie sie der Malware-Forscher Kaffeine als Erstes beim Exploit-Kit Angler beobachtet hat. Dabei schreibt der Exploit den Schad-Code nicht in eine Datei, sondern injiziert ihn als neuen Thread in einen bereits existierenden Prozess, etwa des Browsers, um ihn dort auszuführen.

Die Payload existiert somit nur im Arbeitsspeicher des infizierten Systems. Das hat eine ganze Reihe von Vorteilen: Antiviren-Software arbeitet hauptsächlich dateiorientiert. Sie überwacht vor allem das Ausführen und das Schreiben von Dateien. Gibt es keine Datei mit dem Schad-Code, läuft dieser Schutz ins Leere. Darüber hinaus wird es auch deutlich schwerer, Samples und somit Analysen der Payloads zu erstellen.

Der offensichtliche Nachteil dateiloser Schädlinge: Wird der Host-Prozess beendet, hat der Angreifer seine Bastion auf dem Computer des Opfers verloren. Um das zu vermeiden, kann sich die Payload etwa in eine Windows-Funktion einklinken, die beim Beenden des Prozesses aufgerufen wird. Darüber hinaus gibt es auch dateilose Payloads, die sich in der Registry verankern und so sogar einen Neustart des Computers überleben.

Die Landing-Page

Nachdem sich der Nutzer eines Exploit-Kits für eine oder mehrere Payloads entschieden und diese komfortabel über die grafische Oberfläche hochgeladen hat, kann er sich einen Link erstellen lassen. Der führt auf eine sogenannte Landing-Page. Diese Webseite wird von den Anbietern der Exploit-Kits automatisiert gebaut und bereitgestellt. Hier findet die Suche nach Sicherheitslücken im Browser, die Aktivierung des passenden Exploits sowie die an-

Glossar

Crimeware: Der Begriff bezeichnet Malware, welche zur finanziellen Bereicherung des Angreifers programmiert wurde. Zu ihren Einsatzbereichen gehört das Ausspähen vertraulicher Daten, der Aufbau von Bot-Netzen oder das Verschlüsseln von Dateien zum Zweck der Erpressung (siehe Ransomware).

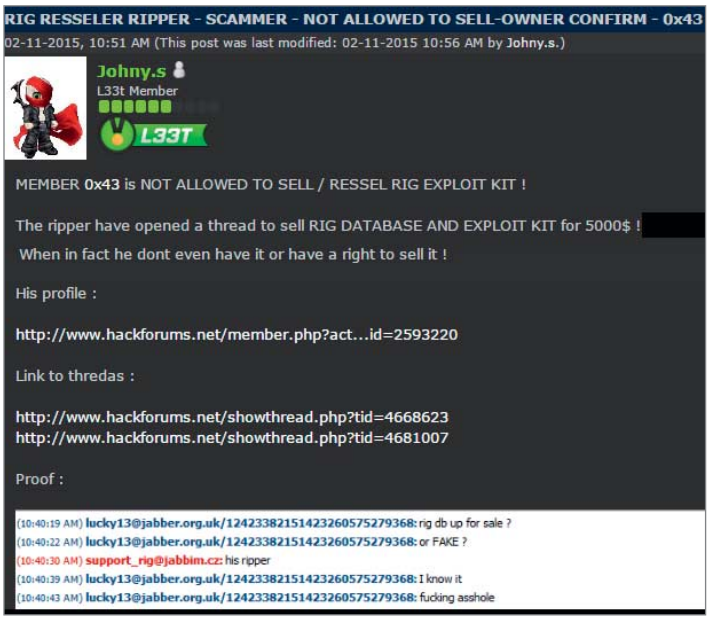
Auch indirekt lässt sich mit Crimeware in Form von Dienstleistungen Geld verdienen. Exploit-Kits und die Crimeware-Kits zur Erstellung eigener Schadsoftware sprechen Kunden an, die auch ohne technisches Know-how Geld durch Cyber-Crime wollen. Das Geschäftsmodell „mietbarer" Crimeware wird häufig als Crimeware-as-a-Service (CaaS) bezeichnet.

Exploit: Über einen Exploit lassen sich Sicherheitslücken in Software oder einem System ausnutzen, um sich unberechtigten Zugriff zu verschaffen. Die betreffenden Schwachstellen werden mittels Programmcode beziehungsweise einer in einem Skript gebündelten Abfolge von Befehlen angegriffen. Damit kann der Angreifer unbemerkt weiteren Schad-Code auf dem System platzieren und ausführen, Daten auslesen oder Admin-Rechte erlangen, etwa um dauerhaften Fernzugriff sicherzustellen.

Bekannte Sicherheitslücken werden mit standardisierten Namen in die sogenannte CVE-Liste (Common Vulnerabilities and Exposures) aufgenommen. Sieht man von 0-Day-Exploits – bisher unbekannten, ungepatchten Lücken – einmal ab, so kann man sich durch regelmäßige Updates und die standardmäßige Deaktivierung anfälliger Komponenten (Flash, Java etc.), die Benutzerkontensteuerung von Windows sowie verantwortungsbewusstem Verhalten im Internet gut vor Angriffen schützen.

Payload: Im Zusammenhang mit Exploit-Kits bezeichnet der Begriff Payload den Schad-Code, welcher nach einem erfolgreichen Angriff auf dem Zielrechner installiert oder ausgeführt wird.

Ransomware: Wie der englische Begriff „Lösegeld" bereits andeutet, handelt es sich hierbei um erpresserischen Schad-Code. Dabei werden Dateien auf dem Zielrechner verschlüsselt und/oder der Zugang mit einem Lockscreen blockiert, um Geld zu erpressen. Die Zahlung erfolgt meist über anonyme Web-Bezahldienste wie Bitcoin.



„L33t Member" Johny.s reagiert wütend auf den versuchten Quellcode-Verkauf des Resellers 0x43.

schließende Infektion mit dem vom Angreifer gewählten Schad-Code statt.

Für die statistische Darstellung im Web-Frontend des Exploit-Kits sammelt die Landing-Page zudem Informationen über den geografischen Standort, die Browser-Version und das Betriebssystem der Angegriffenen. Diese Informationen schickt die Landing Page an den Exploit-Kit-Server, von dem sie im Gegenzug den Exploit und schließlich die Payload bezieht.

Die auf dem vom Exploit-Kit-Team betriebenen Server befindliche Landing-Page wird oft auch von anderen Gangs genutzt. Außerdem kommuniziert dieser Server bereits direkt mit den Systemen, auf denen sich die Kronjuwelen finden, also die Exploits und Payloads. Dessen Adresse wollen die Gangster deshalb nicht mit millionenfach verschickten Spam-Mails in die Welt hinausposaunen.

Um die einzelnen Angriffskomponenten gut abzuschotten, werden den Opfern also typischerweise nicht direkt die Adressen der Landing-Pages präsentiert, sondern vorgeschobene Webseiten, die lediglich auf die Landing-Page umleiten. So kann jede Gang ihre eigenen Frontend-URLs verwenden. Wird der nur kurzfristig aktive Redirect wieder abgeschaltet, führt keine direkte Spur mehr zum wertvollen Host der Landing-Page.

Malvertising

Die Verbreitung des Links zum Redirect-Server kann wie im beschriebenen Szenario per E-Mail erfolgen. Eine weitere Möglichkeit ist das Einfügen von iFrames auf kompromittierten Websites. Die lädt der Browser eines Webseiten-Besuchers beim Aufruf der legitimen Webseite unbemerkt mit. Alternativ bauen die Exploit-Kit-Anbieter beziehungsweise -Käufer eigene Dummy-Webseiten um ihre Landing-Pages herum. Für den benötigten Traffic sorgen dann etwa SEO-Spezialisten, die diese Seiten für beliebte Suchbegriffe bei Google & Co optimieren.

Eine zunehmend eingesetzte Methode zur Weiterleitung auf die Landing-Page heißt „Malvertising". Besonders gefährlich an dieser Technik ist, dass dabei vertrauenswürdige Seiten mit viel Traffic zur Weiterleitung auf die Exploit-Seiten missbraucht werden. Dies geschieht in Form von Werbeanzeigen unauffälligen Inhalts, die von den Kriminellen geschaltet werden. Früher geschah dies vor allem über kompromittierte Anzeigen-Server. Doch mehr und mehr bezahlen die Angreifer tatsächlich für das Einblenden ihrer bösartigen Anzeigen. Das ist einfacherer, als in Server einzubrechen.

Beim Besuch der Webseite mit der Anzeige wird meist direkt auch das Exploit-Kit aktiv. Letztlich wird dabei in einem iFrame dessen Landing-Page geladen. Weniger auffällig sind herkömmliche Werbebanner, die erst aktiv werden, wenn sie der Besucher anklickt. Diese Methode bringt zwar weniger direkte Infektionen, bleibt dafür aber länger unentdeckt. Zwei aktuelle Beispiele für erfolgreiches Malvertising sind die zur Verbreitung des „HanJuan EK" geschalteten Anzeigen auf stark frequentierten Websites wie nydailynews.com, metacafe.com oder dailymotion.com im Februar und März sowie die Verwendung von Googles Ad-Server Doubleclick zur Verbreitung des Exploit-Kits Nuclear im April dieses Jahres.

Vom Vertrauten zum Verräter

Einen interessanten Blick darauf, wie es in der Szene zugeht, gibt die Geschichte vom Aufstieg und Fall des RIG-Exploit-Kits, das 2014 hinter Sweet Orange, Angler und Magnitude Platz 4 in der Verbreitungsstatistik von Trend Micro erreichte.

Ab April 2014 preisen die vermutlich russischen Entwickler ihre Neuentwicklung vor allem im Forum exploit.in an, in dem auch etablierte Exploit-Kits wie Sweet Orange oder das Neutrino Pack gehandelt werden. Statt die Software zu verkaufen, operieren sie konsequent nach dem Modell „Crimeware-as-a-Service": Interessierte können die Software ausschließlich als Komplettpaket mieten; für etwa 30 US-Dollar pro Tag, 150 pro Woche oder 500 pro Monat. Die Zahlung erfolgt dabei anonym über die Krypto-Währung Bitcoin.

RIG gewinnt schnell einen beachtlichen Kundenkreis. SpiderLabs schätzt Anfang 2015, dass die RIG-Entwickler etwa 360 Direktkunden haben. Darüber hinaus hat Trustwave zwei große Reseller ausgemacht, die etwa 250 weitere Kunden beisteuern. Solche

Vom Saulus zum Paulus: Unter dem Namen ExploitKitsMustDie gab sich ein Ex-Reseller des RIG-Exploit-Kits als Anti-Malware-Aktivist.

Reseller können die Daten ihrer Kunden als Administratoren eines RIG-Exploit-Kit-Servers selbst verwalten und agieren somit in hohem Maße unabhängig.

Ausgerechnet das für die Entwickler sehr lukrative Reseller-Modell leitet letztlich das vorläufige Ende des Shooting-Stars unter den Exploit-Kits ein: Im Februar 2015 taucht plötzlich ein neuer Reseller mit dem Nickname 0x43 auf, der bald durch seltsame Preise und dubiose Angebote auffällt. So offeriert er für 5000 US-Dollar auch den kompletten Quellcode inklusive Datenbank des Exploit-Kits. Schließlich schreitet sogar RIG-Entwickler Johny.s ein und stellt klar, dass 0x43 kein autorisierter Reseller sei.

Als kurz darauf auch noch Berichte von Kunden die Runde machen, nach denen 0x43 ihre Payloads durch eigene ersetzt und ihnen damit die infizierten Systeme gestohlen habe, war 0x43 erledigt.

In Rekordzeit vollzieht er einen Wandel zum Anti-Malware-Aktivisten und eröffnet unter dem Namen ExploitKitsMustDie einen Twitter-Account, um sich angeblich auf die Seite der Guten zu schlagen. Im Zuge seines Rachefeldzugs veröffentlicht er darüber schließlich den RIG-Sourcecode. Im ebenfalls veröffentlichten Datenbank-Dump finden sich prompt jene Nutzer wieder, denen 0x43 einige Wochen zuvor den RIG-Zugang verkauft hatte.

Die RIG-Crew war angeschlagen, doch noch nicht am Ende. Bereits drei Tage nach dem Code-Leak lassen die Entwickler verlauten, es habe sich um „alten Code“ gehandelt und es gebe bald eine neue Version. Wahrscheinlicher ist, dass die Entwicklung des Nachfolgers RIG 3.0 erst aufgrund des Leaks in Angriff genommen wurde. Jedenfalls sind die RIG-Entwickler heute wieder im Geschäft. Für 400 statt 150 Dollar pro Woche können Interessenten eine neue Version testen, die vor allem mit aufwendigeren Statistiken aufwartet. Der folgende Artikel wirft einen genaueren Blick auf die geleakte RIG-Version, die alle typischen Komponenten eines hochwertigen Exploit-Kits enthält. (ju@ct.de)

Exploit-Kits im Überblick

Das erste kommerziell vertriebene Exploit-Kit überhaupt, das sogenannte „WebAttacker Kit“, erschien 2006. Gemessen an heutigen Preisen war es ein Schnäppchen: 15 US-Dollar betrug damals der Kaufpreis. Schon mit dem Erscheinen des zweiten, ebenfalls von Russen entwickelten Exploit-Kits änderte sich die Preispolitik radikal: Zwischen 5000 bis 10 000 Dollar betrug der Kaufpreis von mPack. Es bot viel detailliertere Statistiken als sein Vorgänger und neben technischem Support auch monatliche Updates.

Dieses Mehr an Service zog trotz des hohen Preises viele Käufer an – eine Rechnung, die bis heute aufgeht. In den Folgejahren stieg die Anzahl der auf dem Schwarzmarkt verfügbaren Exploit-Kits ebenso rasant wie die Zahl der Malware-Infektionen, die mit Hilfe dieser Werkzeuge verursacht wurden.

Erfolgreiches Mietmodell

2009 beobachtete Symantec die ersten Angebote von Exploits-Kits „as a Service“, bei denen sich die Lizenzkosten an der Nutzungsdauer orientieren. Der bekannteste Vertreter dieses Geschäftsmodells – und zugleich das bis dato erfolgreichste Kit überhaupt – ist das 2010 eingeführte Blackhole Exploit-Kit, welches 2011 einen Marktanteil von über 40 Prozent erreichte und seine führende Stellung in den folgenden Jahren behaupten konnte.

Die Verhaftung des Blackhole-Entwicklers Paunch im Oktober 2013 bedeutete das Aus für dessen Weiterentwicklung und leitete in der Szene ein Umdenken ein. Die Anzahl der neu entwickelten Exploit-Kits ging erstmals seit 2010 zurück – ein Trend, welcher sich 2014 noch verstärkte.

Die neue Vorsicht der Exploit-Kit-Entwickler hat dazu geführt, dass zwar weniger, dafür jedoch ausgereiftere Kits veröffentlicht wurden. Dazu gehört neben RIG das ebenfalls seit 2014 angebotene HanJuan Exploit-Kit, welches im Februar 2015 erfolgreich eine 0-Day-Schwachstelle im Flash Player (CVE-2015-0313) zur besonders effektiven Schad-Code-Verbreitung nutzte und ebenso wie Angler in der Lage ist, angegriffene Rechner „dateilos“ zu infizieren.

Der aktuelle Marktführer der Exploit-Kits heißt „Sweet Orange“, angelehnt an die orangefarbene Bedienoberfläche. Seine Beliebtheit verdankt es nicht zuletzt der Tatsache, dass seine Entwickler den Service noch ausgeweitet haben: Neben den Exploits sorgen sie auf Wunsch auch für den benötigten Traffic auf der Landing-Page. Die Entwickler werben mit 150 000 Besuchern täglich. Bei einer garantierten Infektionsrate von 10 bis 25 Prozent entspräche dies mindestens 15 000 Infektionen pro Tag.

Die Kunden zahlen dafür einen wöchentlichen Mietpreis von etwa 1400 US-Dollar. Noch stärker als die RIG-Entwickler achtet die Gang hinter Sweet Orange allerdings auf Geheimhaltung: Der Handel erfolgt lediglich in Untergrundforen, auf die man erst nach persönlicher Einladung zugreifen kann.

Der Trend zur „Klasse statt Masse“ dürfte sich weiterhin fortsetzen: Wenige, dafür jedoch sehr effektiv arbeitende Exploit-Kits werden einer immer exklusiveren Käuferschaft zu steigenden Preisen angeboten.

Die Oberfläche passt zum Namen des aktuellen Marktführers bei den Exploit Kits: „Sweet Orange“.