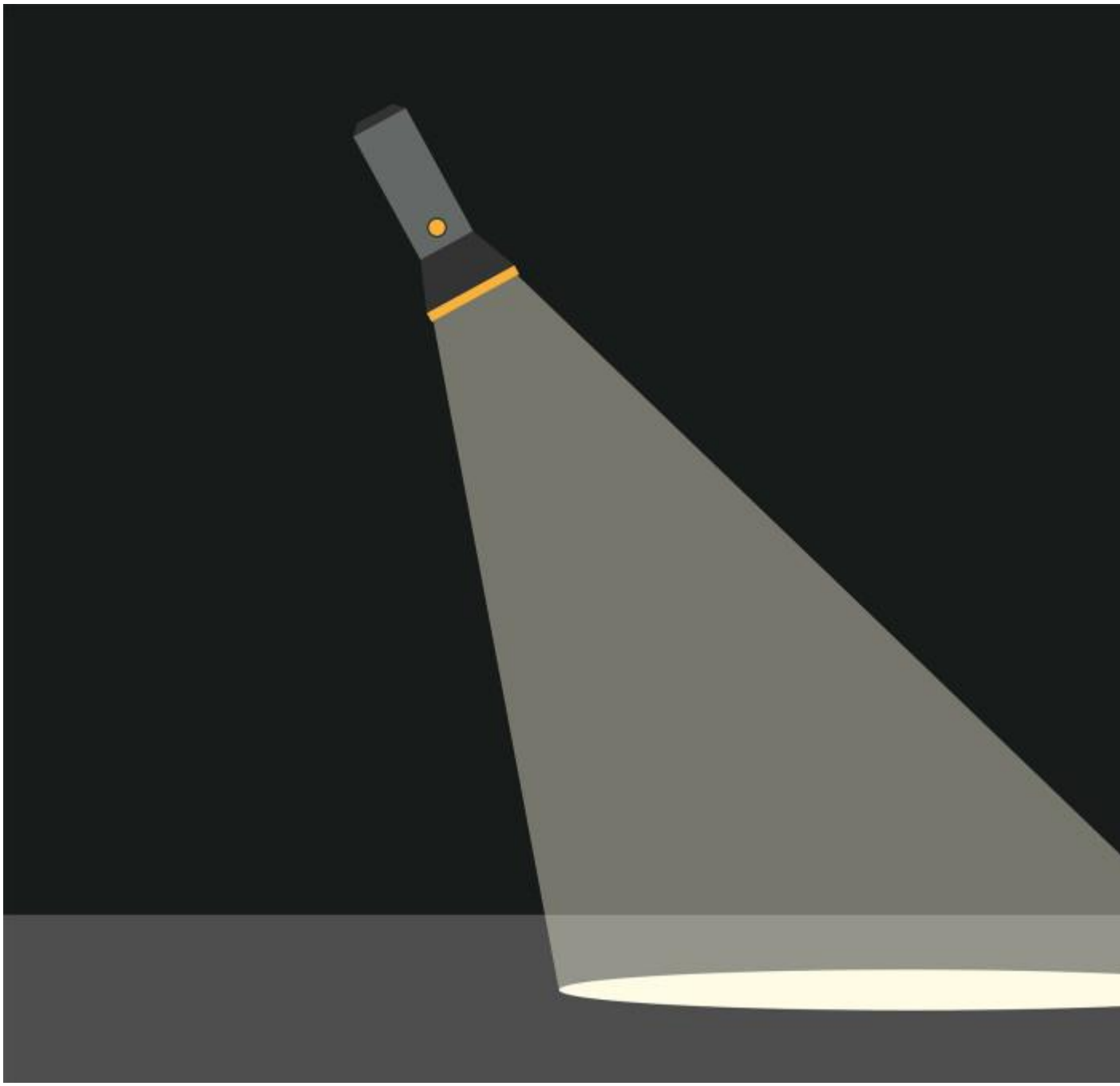
- AUTOR:. KIM ZETTERKIM ZETTER SICHERHEIT
- ERSCHEINUNGSDATUM: 01.13.16.01.13.16
- ZEITPUNKT DER VERÖFFENTLICHUNG: 9.00.9:00 MORGENS

HACKING-TEAMS LEAK GEHOLFEN FORSCHER DIE JAGD NACH EINEM ZERO-DAY-



Klicken Sie auf das Overlay-Galerie öffnen GETTY IMAGES

ZERO-DAY-EXPLOITS SIND eines Hackers bester Freund.Angriffe Ablaufen Schwachstellen in Software, die ohne Wissen der Software-Hersteller sind und daher nicht gepatchten. Kriminelle Hacker und Geheimdienste verwenden Zero-Day-Exploits, um einen Stealth Tür in Ihr System zu öffnen, und weil Antivirus-Unternehmen auch nicht über sie wissen, können die Heldentaten unentdeckt Jahren verbleiben, bevor sie entdeckt sind. Bis jetzt haben sie in der Regel nur durch Zufall aufgedeckt worden. Aber Forscher an Kaspersky Lab haben, zum ersten Mal entdeckt, ein wertvolles Zero-Day-Exploit nach absichtlich gehen auf der Suche nach es. Sie taten also, indem Sie nur die leiseste von Hinweisen, um es zu finden.

Die Malware fanden sie ist ein Remote-Ausführung von Code ausnutzen, dass die Angriffe eine Schwachstelle in Microsofts Silverlight-Software weit verbreitet, ein Browser-Plug-in Netflix und anderen Anbietern verwenden, um zu liefern

Streaming-Inhalte für die Nutzer. Es ist auch in verwendet SCADA und anderen industriellen Steuerungs-Systeme, die in kritischer Infrastruktur und Industrieanlagen installiert sind.
Die Sicherheitslücke, die Microsoft als "kritisch" in einemPatch, um Kunden am Dienstag veröffentlicht, wäre es einem Angreifer ermöglichen, Ihr System nach dem Aufstehen Sie eine bösartige Webseite, auf der Exploit besuchen wohnt-Regel durch eine Phishing-E-Mail, Tricks, die Sie in die Sie auf zu infizieren ein bösartiger Link. Der Angriff funktioniert mit allen Top-Browsern außer Chrome- aber nur, weil Google entfernt Unterstützung für die Silverlight-Plug-in in der Chrome-Browser im Jahr 2014.
Kaspersky Lab fing seine großen Fische, die Silverlight nutzen, Ende November nach der Zero-Day-infizierten Rechner eines Benutzers. Aber es dauerte einen cleveren Verlockungen und Monaten der Patient warten, um diesen Preis zu bekommen. Die Geschichte hinter dieser Entdeckung bietet eine faszinierende Lektion, wie die Forscher möglicherweise mehr null Tage in der Wildnis versteckt aufzudecken.

Hacking-Teams Hacked Emails Angeboten der erste Hinweis

Alles begann mit einem Gespräch, das nie gedacht war öffentlich sein.

Im Juli 2015 ein Hacker nur als "Phineas Fisher" bekannt gezielt die italienische Überwachungsfirma Hacking-Team und stahlen einige 400 GB Daten des Unternehmens, einschließlich interne E-Mails, die er geworfen online. Der Hack freiliegenden Geschäftspraktiken des Unternehmens, aber es zeigte auch, das Geschäft von Zero-Day-Anbietern,die versuchen, ihre Taten zu Hacking Team Markt wurden.Die umstrittene Überwachungsunternehmen, das seine Software für die Strafverfolgung und Geheimdienste in der Umgebung verkauft der welt darunter zu repressiven Regimes wie Sudan, Bahrain und Saudi-Arabien-nutzt Zero-Day-Exploits, um ihre Überwachungsinstrumente zu schleichen auf zielgerichtete Systeme.
Costin Raiu, Leiter der Kaspersky Global Research und Analysis Team, wurde von einem Verhandlungs insbesondere die zwischen Hacking-Team und ein Zero-Day-Verkäufer, der sich selbst als 33-jährige Russe namens Vitaliy Toropov identifizierte im Jahr 2013 stattgefunden fasziniert. In einer Reihe von E-Mails, Online-abgeladen und in einer hervorgehobenen Ars Technica Geschichte über die gehackten Daten, verhandelt der Forscher den erfolgreichen Verkauf eines $ 45.000 Blitz nutzen, um Hacking-Team.
Nach Abschluss der Verhandlungen über das auszunutzen, Toropov, wie alle guten Geschäftsmänner, versuchte, Hacking-Team in mehr von seinen Gütern, die er bereit ist, mit einem Abschlag zu verkaufen für Groß kauft-ein $ 5.000 Rabatt war interessant, wenn Hacking-Team kaufte eine zweite Null Tag ab ihn und ein $ 10.000 Preisnachlass, wenn sie kaufte ein Drittel. Zu seinen Angeboten: "Ich

empfehle Ihnen, die frische 0 Tage für iOS 7 / OS X Safari", schrieb er,"oder meine alte Silverlight nutzen, die vor 2,5 Jahren geschrieben wurde, und hat alle Chancen, um weiterhin in der nächsten Jahre sowie zu überleben."

Raiu war nicht sicher, wie man für die Zero-Day-Exploit zu suchen, da er nicht über Code zu prüfen, und nicht einmal wissen, welche Sicherheitslücke in Silver es gezielt.

Obwohl die iOS-Exploit war interessant war Raiu viel mehr fasziniert von der Silverlight-Exploit, Toropov gesagt hatte unentdeckt blieb seit 2011 Es war keine leere Prahlerei von einem unerfahrenen Newcomer.

Toropov ist ein überaus produktiver Bug Jäger und nutzen Schriftsteller, der bis zum Jahr 2013 war ein aktiver Teilnehmer an Bug Bounty-Programme -Programme, die sich auszahlen Bug Jäger Geld für Informationen über Sicherheitslücken die sie finden, die dann an den Software-Hersteller übergeben, so dass sie die Löcher flicken.Zwischen 2011 und 2013 offen Toropov mehr als 40 Sicherheitslücken zu diesen Programmen, entsprechend einer Tabellenkalkulation hat er im Internet veröffentlicht und eine Seite für seine Entdeckungen auf dem Packet SturmSicherheits Website. Doch im Oktober 2013 seine öffentliche Bekanntgabe von Bugs ausgetrocknet, nachdem er offenbart zwei Schwachstellen in Silverlight zu Microsoft. Im selben Monat ist, als er heimlich die Vermarktung seiner Waren zum Hacking Team darunter offenbar eine Silverlight nutzen, die er von Microsoft, um es für Kunden, die es verwenden, um Systeme zu hacken verkaufen gehalten hatte.
Wenn der Exploit bereits an andere Kunden verkauft worden und wurde zu infizieren Systeme in der Wildnis für zweieinhalb Jahre, wunderte Raiu, ob er in der Lage, es zu finden. Es gab nur ein Problem. Toropov vorgesehen keine Details über den Exploit das könnte ihm helfen, es aufzuspüren.

In der Regel null Tage sind durch Unfall, wenn jemand entdeckt sie gehackt haben und eine forensische Untersuchung ihres Systems deckt Zero-Day-Malware gefunden. Sobald diese Exploits entdeckt, schau Antivirus-Unternehmen für die verräterischen Fingerabdrücke in dem Code, der ihnen helfen kann, suchen Sie die Malware auf anderen Systemen; dann werden sie ihre Unterschriften-Scanner verwenden, um Kundensysteme zu suchen zu schreiben. Aber in diesem Fall, Raiu war nicht sicher, wie man für die Zero-Day-Exploit zu suchen, da er nicht über

Code zu prüfen, und nicht einmal wissen, welche Sicherheitslücke in Silver es gezielt.

Klicken Sie auf das Overlay-Galerie öffnenCostin Raiu, Leiter der Kaspersky-Lab-Global Research und Analysis Team. KASPERSKY LAB

Aber nach einem Blick auf den öffentlichen Liste früherer Bug Entdeckungen Toropov ist, bekam er eine Idee.Er begann die Prüfung der Proof-of-Concept-Exploit Toropov hatte für die Fehler, er würde schon entdeckt, um zu sehen, ob er keine besonderen Programmiertechniken oder Muster in der Art, wie er schrieb, Code, der als Signatur zu Heldentaten finden, verwendet werden könnten, zu finden geschrieben sein, die in der Wildnis sein könnten. Forschern Proof-of-Concept-Exploits zum Bug Bounty-Programme in einem gutartigen, dass die Schwachstellen sie gefunden haben, sind real und können ausgenutzt werden, zu überprüfen. Normalerweise ist die Proof-of-Concept-Code einfach startet die Taschenrechner-Anwendung auf einer Maschine, um visuelle Beweis dafür, dass der Exploit funktionierte bereitzustellen.

Raiu Instinkt über Blick auf die veröffentlichten Dateien richtig war. Er untersuchte insbesondere eine Proof-of-Concept-Code Toropov hatte für eine der Sicherheitslücken von Microsoft Silverlight hatte im Jahr 2013. Unter den Dateien für diesen Exploit veröffentlicht geflickt war eine, die Debugging-Code enthalten. Debugging-Code wird von Entwicklern verwendet, um Fehler im Programm aus, als sie es zu schreiben. Es gab drei besondere Saiten-Debugging-Code, der Raiu Auge, die in mehrere Dateien Toropov schrieb schien gefangen.

"Mit Exploit-Entwickler haben sie [code] Bibliotheken bauen sie, und sie halten die Wiederverwendung sie von einem zu einem anderen zu nutzen, um ihre Arbeit zu vereinfachen," Raiu stellt. "Ich sagte, was ist, wenn seine anderen Silverlight nutzt ähnlich wie diese Proof-of-Concept, die er im Jahre 2013 schrieb, bist?"

MEHR AUF ZERO-DAY-EXPLOITS

- 
  Eine beispiellose Look at Stuxnet, das weltweit erste digitale Waffe

- **Hacker Lexikon: Was ist ein Zero Day?**

- **Hackers Anspruch Million-Dollar Kopfgeld für iOS Zero Day-Angriff**

Programmierer normalerweise Debugging-Code aus den endgültigen Versionen ihrer Programme, aber manchmal sind sie verlassen im Quellcode und kompiliert wird in den binären, auch wenn es nicht Code, der von dem Exploit verwendet wird, um seine Funktionen durchzuführen. Raiu hatte gehofft, dass der Fall war.

Er benutzte ein Werkzeug namens YARA, um zu sehen, wenn er die Spuren der Saiten auf Kaspersky Kundensysteme finden konnte. YARA wurde 2007 von Victor Manuel Alvarez, einer spanischen Sicherheitsforscher, die sich entwickelt, funktioniertVirustotal, eine kostenlose Online-Virenscanner, die Google jetzt besitzt. Mit dem Tool können die Forscher eine sogenannte YARA Regel zu erstellen, für bösartige Dateien in Familien von Malware zu suchen und zu entdecken Mustern in ihnen, um die Gruppe ähnliche Dateien. YARA Regeln können auch verwendet werden, um Netze und Systeme für die gleichen Muster des Codes zu scannen. Das ist, wie Raiu beschlossen, es zu benutzen.
Er hatte versucht, YARA Regeln schon einmal auf diese Weise zu verwenden, aber habe es versäumt, zu finden, was er suchte. Einer der Kunden Kaspersky hatte durch zwei Großtaten, die durch einen infizierten Adobe PDF-Datei kam angegriffen worden. Eine der Taten konnten die Angreifer aus dem Adobe Reader Sandbox-Schutzschicht einige Anbieter stellen in ihrer Software, um Heldentaten

vom Sprung aus einer Anwendung und eine Infektion des Kernsystems zu verhindern zu entkommen. Raiu und seine Kollegen nie gefunden die Heldentaten, aber waren in der Lage, herauszufinden, wie sie arbeiteten und benachrichtigt Anbieter, um die gefährdeten Löcher geflickt zu bekommen.

Trotz dieser früheren Versagen, dachte Raiu es war einen Versuch wert, eine YARA Regel wieder mit Toropov auszubeuten. Im Juli, kurz nach dem Lesen der E-Mails Toropov Austausch mit Hacking-Team, erstellt Raiu ein YARA Regel auf die Debugging-Code, den er gefunden hatte und dann verteilt es an automatischen Exploit Prevention-Tool des Unternehmens und dem Kaspersky SecurityNetwork, von Kunden, die haben zusammen ausgewaehlt mit Kaspersky bösartigen Proben auf ihren Systemen zu teilen. Dann wartete er.

```
rule exploit_Silverlight_Toropov_Generic_XAP {

meta:

    author = "Kaspersky Lab"
    filetype = "Win32 EXE"
    date = "2015-07-23"
    version = "1.0"

strings:


    $b2="Can't find Payload() address"  ascii wide
    $b3="/SilverApp1;component/App.xaml" ascii wide
    $b4="Can't allocate ums after buf[]" ascii wide
    $b5="------------ START ------------"

condition:

    ( (2 of ($b*)) )

}
```

Klicken Sie auf das Overlay-Galerie öffnenDebugging-Zeichenfolgen in der YARA Regel Kaspersky verwendet zu finden, die Silverlight nutzen. Mit freundlicher Genehmigung von Kaspersky Lab

Monate vergingen, und es gab keine Anzeichen einer Infektion für alle Kunden. Raiu schließlich vergaß sein kleines Experiment.

Dann am 25. November eine Infektion plötzlich auf dem Rechner eines Benutzers im Nahen Osten aufgetaucht.Kunden, die in der Unternehmensnetzwerk KSN einverstanden, dass Schadcode auf ihren Maschinen gefunden Kaspersky zur

Analyse geschickt werden.Bemerkenswert ist, ein paar Stunden später, hochgeladen jemand eine Probe des gleichen zu nutzen, um dem Virus Total Website, sondern von einer anderen geografischen Region. Virus insgesamt ist eine Website, mehrere Virenscanner aggregiert, also können Leute verdächtigen Dateien zu veröffentlichen und zu bestimmen, ob sie bösartig. Die Datei wurde von einer IP-Adresse in Laos hochgeladen. Es war am 21. Juli zusammengestellt, Exploit nur ein paar Wochen nach Toropov die E-Mails mit Hacking-Team diskutieren seine Silverlight hatte Online ausgesetzt.

Es dauerte nicht lange, nachdem Raiu und sein Team haben ihre Hände auf bösartigen Code ihrer Kunden, um festzustellen, dass es in der Tat eine Silverlight-Zero-Day-Exploit.

"Diese speziellen Debug Strings waren das einzige, was wir könnten, auf von seiner [früheren] Silver Exploits hängen", sagt er. Chancen waren gegen seinen Gamble Arbeits; aber es tat.

Seitdem hat sich Kaspersky nicht aufgedeckt alle anderen Proben auf Kundenmaschinen, die wer auch immer wurde mit der Exploit wurde mit es vernünftig, nur bestimmte Opfer Ziel schlägt. Die Tatsache, dass zwei Opfer in verschiedenen Teilen der Welt waren offenbar am selben Tag getroffen schlägt der Angreifer wurde eine Kampagne an diesem Tag Targeting verschiedenen Opfer zugleich. Raiu schätzt den Exploit wert war zwischen $ 20.000 und $ 40.000 auf der Zero-Day-Markt.

WIRED streckte die Hand aus, um Toropov über den Exploit zu fragen, ob er es geschrieben hatte, und reichte ihm die technische Beschreibung, die Kaspersky hatte zu der Sicherheitsanfälligkeit es zielt-eine schriftliche Binary Bug in der Silverlight-Software. Er sagte, er sei nicht mit der Schwachstelle vertraut.
"Ich habe nicht [wissen] über diese besondere Binary bug", schrieb er in einer Botschaft an WIRED. Er fragte, ob der Exploit mitgelieferten Code aus einer seiner früheren Heldentaten, und wenn gesagt, dass es tat, fragte er, um sie zu sehen. WIRED schickte ihm den Code nach Microsoft hatte schon seinen Patch für die Sicherheitslücke verteilt.

"Ich möchte diese 0 Tage, aber leider ist es nicht von mir", sagte er nach Prüfung es. "Wie auch immer, es war interessant, die Teile meines calc poc in diesem Shellcode zu finden, thanks for sharing."

Sein Begriff "calc poc" bezieht sich auf den Rechner Proof-of-Concept-Code, den er im Jahr 2013 für das vorangegangene Silverlight Anfälligkeit Microsoft hatte dann wieder geflickt veröffentlicht hatte.

Toropov habe nicht gesagt, warum Proof-of-Concept-Code schrieb er wurde zeigt sich in ein Exploit er sagt, er habe es nicht geschrieben, aber er sagte, er sei nicht überrascht, wenn es in der Exploit Kaspersky gestellt sehen. Gefragt, ob er jemals verkauft Hacking-Team beendete das Silverlight nutzen, die er in seinem 2013 email bot ihnen, er sagte nein.

Raiu sagt, es macht keinen Sinn, dass jemand anderes würde Toropov öffentlichen Proof-of-Concept-Code in ihren Exploit gesetzt haben, aber es ist nicht in Frage. Er sah es in mindestens einem anderen Fall passieren, wenn jemand verwendet, Teile der Proof-of-Concept-Code Toropov für das Jahr 2013 Silver Anfälligkeit er Microsoft offenbart hatte, schrieb, und verwendet werden, dass als Baustein zu schaffen ein Exploit.

Ob der Exploit wurde von Toropov geschrieben, hält Raiu seiner Jagd nach ist es ein großer Erfolg zu sein, da es eine weniger Zero-Day-Schwachstelle verfügbar für Angreifer ausnutzen.

"Das ist eigentlich das erste Mal, dass wir in Fang etwas, das wir auf der Jagd geplant gelingt", sagt Raiu. "Es war wahrscheinlich ein bisschen Intuition und Glück. Wenn der Compiler diese [Debugging] Zeichenfolgen entfernt haben, so ist offenbar [hätte es] kein Glück für mich. "

Aber jetzt, dass die Technik hat sich bewährt, kann es möglich sein, Code aus anderen Toropov Exploits, um zusätzliche Null Tage, die möglicherweise es aufzudecken zu untersuchen. Und wenn es ähnliche verräterische Anzeichen im öffentlichen Code anderer Forscher, dies kann verwendet werden, um mehr Zero-Day-Exploits sowie aufzudecken werden.

Zurück zum Anfang.Direkt zu: Start des Artikels.

- ABENTEUER
- HACKING-TEAM
- HACKS UND CRACKS
- SILVE