Wie Nordkorea die Hacks nachgewiesen werden

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion–hide“>zurück zum Artikel <figure class=„printversionlogo“></figure><figure class=„aufmacherbild“><figcaption class=„akwa-caption“><p class=„caption akwa-captiontext“>Riesige Statuen von Kim Il Sung und Kim Jong Il. Die verstorbenen Despoten werden in der Erbdiktatur als Übermenschen verehrt. <p class=„source akwa-captionsource“>(Bild: gemeinfrei) </figcaption></figure> „Hidden Cobra“ ist der US-Codename für die staatlichen Hacker Nordkoreas. Wie kann man überhaupt wissen, ob und wann die Diktatur hinter einer Attacke steckt? „Das FBI hat heute mitgeteilt, und wir können es bestätigen, dass Nordkorea sich an dieser Attacke beteiligt hat“, sagte Ende 2014 der damalige US-Präsident Barack Obama. Er bezog sich dabei auf flächendeckende Angriffe auf Server von Sony Pictures im November des Jahres, bei denen umfangreich Daten gestohlen worden waren. Doch wie können die Ermittler wissen, wer hinter einem Hack steht? Ein Vortrag von McAfee-Experten auf der CanSecWest 2020 vergangene Woche in Vancouver gewährte Einblick in deren Detektivarbeit. Ryan Sherstobitoff und Thomas Roccia von McAfee Advanced Threat Reserach studieren seit sechs Jahren die Arbeit der Nordkoreaner. Das dabei gewonnene Wissen hilft ihnen, die Angreifer aufzuspüren: „Die meisten Attacken der Hidden Cobra beginnen mit Spear-Phishing.“ Hidden Cobra ist der von US-Behörden genutzte Codename für „everything cyber North Korea“, also jegliche digitale Konfliktführung Nordkoreas. Sie soll spätestens 2007 begonnen haben. Bei Spear-Phishing wird keine technische Schwachstelle ausgenutzt, sondern eine menschliche: Unter einem Vorwand entlocken Angreifer Zielpersonen deren Zugangsdaten. <article class=„a-article-teaser a-article-teaser–horizontal-layout-small a-u-no-margin-bottom articleboxarticle-teaser“> <figure class=„a-article-teaserimage-container“> <noscript> <img alt=„Barack Obama “ class=„c1“ src=„https://heise.cloudimg.io/width/200/q50.png-lossy-50.webp-lossy-50.foil1/_www-heise-de_/imgs/18/2/8/6/6/2/0/9/Screenshot_2014-12-19_at_15-1ab19294629582c8.png“ srcset=„https://heise.cloudimg.io/width/200/q30.png-lossy-30.webp-lossy-30.foil1/_www-heise-de_/im

gs/18/2/8/6/6/2/0/9/Screenshot_2014-12-19_at_15-1ab19294629582c8.png 2x“/> </noscript> </figure> [1]</article> Nun ist Spear-Phishing ein Indiz, das auch auf viele andere Täter zutrifft. Weitere Merkmale, die die beiden Forscher gefunden haben, schließen aber schon fast alle nicht-staatlichen Banden aus: „Es sind gut organisierte, aggressive Angreifer. Sie betreiben Cyberspionage, Sabotage und andere Cybercrime-Kampagnen“, so die McAfee-Experten, „Sie updaten ihre Werkzeuge und ihr Arsenal seit mehr als einem Jahrzehnt.“ Nicht-staatliche Täter haben selten so langen Atem und sind auch kaum auf Sabotage aus. <figure class=„a-u-inline-left a-inline-image a-u-inline“> <figcaption class=„a-caption“> Dragos Ruiu, Veranstalter der kanadischen IT-Security-Konferenz CanSecWest (Bild: Daniel AJ Sokolov) </figcaption></figure><h3 class=„subheading“ id=„nav_kompilierter0“>Kompilierter Code mit identischen Strings</h3> Besonders verräterisch: „Verschiedene Gruppen innerhalb der Hidden Cobra arbeiten mit der selben Malware-DNA auf unterschiedliche Ziele hin.“ Mehrere Familien implantierter Malware [2] haben über die Jahre gleichen Code genutzt: „Software aus der selben Familie, die in der selben Entwicklungsumgebung kompiliert wurde, kann eine signifikante Menge identischer Zeichenfolgen aufweisen“, erläuterte Roccia, „Es gibt aber nicht nur gleichen Code, sondern auch gleiche Funktionsweisen.“ Solche Übereinstimmungen weisen auf dieselbe Quelle hin. Weitere Übereinstimmungen, die McAfee gefunden hat: Gemeinsam genutzte Infrastruktur, wiederverwendete IP-Adressen, wiederverwendete Makros und gemeinsam genutzte, gefälschte TLS-Zertifikate. Diese Zertifikate halfen den Forschern übrigens bei der Bekämpfung einer Operation Sharpshooter genannten weltweiten Kampagnen Nordkoreas der Jahre 2018 und 2019. Die Täter hatten fremde, kompromittierte Server als Command & Control Server genutzt, und chinesische Webshells sowie ExpressVPN, um Spuren zu verwischen. Weil aber dieselben gefälschten Zertifikate mehrfach verwendet wurden, konnte McAfee Advanced Threat Research weitere Command & Control Server der Nordkoreaner aufspüren, wo dann auch Malware von früheren nordkoreanischen Kampagnen auftauchte. <h3 class=„subheading“ id=„nav_gleiches_backend_1“>Gleiches Backend</h3> Dabei zeigte sich, dass die Nordkoreaner für viele ihrer Operationen ein spezifisches Backend-Framework verwenden. Ursprünglich in Python programmiert, tauchten später auch ASP.NET-Versionen auf. Stets gab es eine mehrstufige Weiterleitung von Befehlen zu einem Master Server. Ein weiterer Hinweis ist ein spezifisches HTTP-Request-Format, das die Täter einsetzen. Es führt sogar „Nordkoreanisch“ als akzeptierte Sprache an. Geholfen hat den Forscher übrigens eine von den Angreifern selbst erstellte Datei namens Vendor.php: Sie enthielt stets eine Whitelist mit IP-Adressen jener Clients, die den Command & Control Server steuern dürfen. <article class=„a-article-teaser a-article-teaser–horizontal-layout-small a-u-no-margin-bottom articleboxarticle-teaser“> <figure class=„a-article-teaserimage-container“> <noscript> <img alt=„Federal Reserve Bank of New York“ class=„c1“ src=„https://heise.cloudimg.io/width/200/q50.png-lossy-50.webp-lossy-50.foil1/_www-heise-de_/imgs/18/2/8/6/6/2/0/9/2013_Federal_Reserve_Bank_of_New_York_from_Maiden_Lane_top-

a9b458b57c4070ec.jpeg“ srcset=„https://heise.cloudimg.io/width/200/q30.png-lossy-30.webp-lossy-30.foil1/_www-heise-de_/imgs/18/2/8/6/6/2/0/9/2013_Federal_Reserve_Bank_of_New_York_from_Maiden_Lane_top-a9b458b57c4070ec.jpeg 2x“/> </noscript> </figure> [3]</article> Unter den Überbegriff Hidden Cobra fallen verschiedene digitale Bataillone der Diktatur. Sie haben Bezeichnungen wie Guardians of Peace, ZINC oder Nickel Academy erhalten. Private Sicherheitsfirmen verwenden andere Namen, zum Beispiel Lazarus, Bluenoroff, APT37 oder Kimsuky. Jeder dieser Gruppen verfolgt unterschiedliche Ziele im Dienste Nordkoreas. <h3 class=„subheading“ id=„nav_alle_staaten2“>Alle Staaten machen Cyberscharmützel</h3> Grundsätzlich betreibe fast jeder Staat ein Programm für aggressives Verhalten in Datennetzen auf die eine oder andere Weise, erklärten die Vortragenden. Vorteile gegenüber klassischer Gewaltanwendung seien die geringeren Kosten, leichteres Leugnen, und dass weltweit zugeschlagen werden könne. In der Regel sollen die staatlichen Aktionen bestimmte staatliche Ziele unterstützen. Diese können politischer, außenpolitischer, militärischer, oder finanzieller Natur sein oder direkt der Beeinflussung von Menschen oder Organisationen dienen. Nordkorea reagiere mit digitalen Attacken oft auf internationale Sanktionen. Außerdem würden regelmäßig Oppositionelle und „Staatsfeinde“ angegriffen, sowie humanitäre Organisationen, die über Menschenrechtsmangel in Nordkorea berichten. Zudem versuche das Land, sich durch Hacking fremde Militärtechnik zu beschaffen. Mit solchen Verbrechen sind die Nordkoreaner leider nicht alleine. Doch ein weiteres Tatbild ist für Staaten selten: „Sie umgehen Sanktionen, indem sie sich an Kryptowährungen sowie digitalen Bankräuben beteiligen“, berichtete Sherstobitoff. Man sieht: Die Zuordnung einer Attacke beruht auf umfangreichem Vorwissen, erworben durch jahrelange Beobachtung und forensische Untersuchungen gehackter Systeme. Die Wiederverwendung von Code, Zertifikaten und Systemen, aber auch Vorgehensweisen, Ziele und Motive ergeben zusammen ein Bild, das je nach Situation mehr oder weniger deutlich auf die Täterschaft schließen lässt. Auf eine für eine strafrechtliche Verurteilung ausreichende Beweisführung kommt es in der geopolitischen Arena ja nicht an. Geheimdienste können überdies auf Informationen zurückgreifen, die privaten Forschern wie Roccia und Sherstobitoff nicht zugänglich sind. Siehe dazu auch den Hintergrund-Artikel über Attribution: <ul class=„rtelist rtelist–unordered“>
Hacker-Jagd im Cyberspace: Grundlagen und Grenzen der Suche nach den Tätern [4] () <hr/> URL dieses Artikels:
<small>

```
https://www.heise.de/-4687909
```

</small> Links in diesem Artikel:
<small>

```
<strong>[1]</strong> https://www.heise.de/meldung/Sony-Hack-Obama-kuendigt-Vergeltung-an-2504931.html
```

</small>
<small>

```
<strong>[2]</strong> https://www.heise.de/thema/Malware
```

</small>
<small>

```
<strong>[3]</strong> https://www.heise.de/meldung/Milliarden-Coup-in-NY
```

```
-Zentralbank-Konto-per-Ueberweisung-geleert-3131832.html
```

</small>
<small>

```
<strong>[4]</strong> https://www.heise.de/select/ct/2017/14/14990302135
70537
```

</small>
<small>

```
<strong>[5]</strong> mailto:ds@heise.de
```

</small>
 Copyright © 2020 Heise Medien </html>