Fidelis Cybersecurity

BLOG

Die neue Ära der Ransomware nach GandCrab

Fabio Slomp – Fidelis Cybersecurity GmbH

Bedrohungsinformationen und -analysen

Die neue Ära der Ransomware nach GandCrab

Im Juni 2019 beendeten die Malware-Entwickler von GandCrab ihre kriminellen Kampagnen für diesen namensgebenden Ransomware-Stamm, der in den vergangenen eineinhalb Jahren zu einer der produktivsten Ransomware-Familien geworden war. Seither gibt es zahlreiche Untersuchungen und Berichte zu den Herausforderungen der neu entstandenen Ransomware-Angriffe. In jüngster Zeit konnten einige von diesen Angriffsvarianten mehr Interesse wecken als andere – sei es aufgrund bekannt gewordener und medienwirksamer Vorfälle oder sei es aufgrund der zunehmenden Nutzung beliebter Malware-Gattungen und -Kits in einem relativ kurzen Zeitraum. Zu diesen gehören beispielsweise Sodinokibi, Eris und Robbinhood.

Untersuchungen deuten darauf hin, dass Sodinokibi – entdeckt im April 2019 – möglicherweise mit GandCrab in Verbindung gebracht werden kann. Bereits im Juni 2019 wurde berichtet, dass mehrere Regierungsbehörden in Texas betroffen waren. Eris hat in jüngster Zeit großes Interesse bei mehreren Entwicklern von Commodity-Malware-Kits ausgelöst. Hierzu zählen die RIG- und Lord Exploit Kits (EKs). Auch Robbinhood war in den vergangenen Monaten die Ursache für mehrere Ransomware-Angriffe auf öffentliche Verwaltungen und kommunale Einrichtungen.

Die wichtigsten Erkenntnisse:

- Die Popularität von Sodinokibi hängt möglicherweise mit der vermuteten Beziehung zu GandCrab zusammen.
- Ungewöhnliche Stämme wie Robbinhood und Eris können immer noch erhebliche Schäden anrichten und werden auch künftig von weit verbreiteter Commodity-Malware und Exploit-Kits eingesetzt.
- Phishing-E-Mails sind nach wie vor der beliebteste Angriffsvektor. Dabei erfordern die Schwachstellen in der Software und den Diensten wie beispielsweise Oracle WebLogic nur eine minimale oder auch keine Interaktion der Nutzer, sprich der Opfer.
- Ältere Schwachstellen in weit verbreiteter Software und in populären Diensten werden auch weiterhin bevorzugt ausgewählt und ausgenutzt.

Sodinokibi oder auch „REvil“

Die Sodinokibi Ransomware, auch „REvil“ genannt, wurde erstmals im April 2019 aufgedeckt und beschrieben. Seit der ersten Berichterstattung haben weitere Untersuchungen mehrere Ähnlichkeiten zwischen Sodinokibi und GandCrab erkannt. Trotz der kurzen zeitlichen Überschneidung mit dem mutmaßlichen Vorgänger wird Sodinokibi beliebter. Im zweiten Quartal 2019 war Sodinokibi einer der beliebtesten Ransomware-Stämme, der von Analysten beobachtet wurde, und machte 12,5 Prozent des Ransomware-Marktanteils aus. Im Vergleich: Ryuk lag bei 23,9 Prozent, Phobos bei 17,0 Prozent und Dharma bei 13,6 Prozent. In diesem Zeitraum – und dies könnte ein weiterer Beleg für die Verbindung zu den GandCrab-Entwicklern sein – überstieg Sodinokibi den GandCrab-Marktanteil von 10,2 Prozent sogar. Allerdings gilt es dabei auch zu berücksichtigen, dass die GandCrab-Aktionen bereits abnahmen und diese kriminelle Organisation ihre Tätigkeiten rund um GandCrab Ende Juni 2019 einstellte.

Die Sodinokibi Ransomware wurde erstmals durch die Ausnutzung einer Zero-Day-Schwachstelle (CVE-2019-2725) auf einem Oracle WebLogic Server entdeckt. Dies war – verglichen mit den meisten generischen Ransomware-Stämmen – einzigartig, da die Ausnutzung dieser Server-Schwachstelle keine Benutzerinteraktion erforderte, wie dies wie bei Phishing-Mails üblich ist. Erst im Juni 2019 wurde beobachtet, dass das RIG Exploit Kit Sodinokibi für eine ältere Microsoft Win32k-Schwachstelle (CVE-2018-8453) nutzt. Seit dem Wiederaufleben der Exploit Kits in jüngster Zeit ist das RIG Exploit Kit ist eines der gängigsten Malware-Artefakte. Wird die Malware in ein Exploit Kit integriert und angepasst – wie dies bei dem bekannten Exploit Kit RIG der Fall ist – kann dies zu einer starken Zunahme der Sodinokibi-Kampagnen und -Angriffe führen. Dies wurde am 19. August besonders deutlich als berichtet wurde, dass mehrere staatliche Regierungsbehörden in Texas von einem Ransomware-Angriff betroffen waren, der auf Sodinokibi zurückzuführen war.

Eris

Eris ist ein weniger bekannter Ransomware-Stamm, der bei anderer gängiger Commodity-Malware immer beliebter wird. Am 29. Juni 2019 veröffentlichte Eris, ein Nutzer des russischsprachigen Exploit.in-Forums, einen Thread, der für die Funktionalitäten dieser neuen, gleichnamigen Ransomware warb. Zwischen dem 29. Juni und dem 5. Juli veröffentlichte Eris weitere Beiträge zu den Funktionen der Eris Ransomware und zu den Möglichkeiten für Tutorials und für ein Partnerprogramm. Sicherheitsanalysten konnten die Eris Ransomware jedoch bereits seit Mai 2019 „in freier Wildbahn“ beobachten.

Anfang Juli 2019 trat Eris bereits in dem beliebten RIG Exploit Kit auf. Zwischen Juli und August 2019 wurde Eris aus der Azera Drive-by Malware und dem Lord Exploit Kit gestrichen nachdem die Adobe Flash Use-after-Free-Schwachstelle (CVE-2018-15982) bereits ausgenutzt worden war.

Robbinhood

Die Robbinhood Ransomware ist ein weiterer Stamm, der im Vergleich zu anderen beliebten Varianten eher selten auftritt. Die geringere Verbreitung ist darauf zurückzuführen, dass die Ransomware einen hohen Bekanntheitsgrad aufgrund gravierender, medienwirksamer Vorfälle in Greenville (NC) im April 2019 und dann Baltimore (MD) im Mai 2019 erlangte. In beiden Fällen legte Robbinhood die Systeme der Kommunalverwaltung für mehrere Wochen lahm, sodass wichtige kommunale Leistungen über mehrere Wochen hinweg nicht mehr erbracht werden konnten.

Obgleich der ursprüngliche Angriffsvektor noch immer fraglich ist, ist davon auszugehen, dass Robbinhood die betroffenen Systeme über das Remote-Desktop-Protokoll (RDP) infiziert hat oder über andere Malware heruntergeladen wurde. Robbinhood wird auch weiterhin ein Ransomware-Stamm sein, vor dem man sich in Acht nehmen sollte – insbesondere im öffentlichen Sektor.

Die Gemeinsamkeiten der Ransomware-Familien

Während unserer Forschungsarbeit konnten wir feststellen, dass mehrere Ransomware-Familien – sowohl die generischen als auch die weiterverwendeten – oft ähnliche Prozesse und Verhaltensmuster vorweisen, die auf den infizierten Hosts ausgeführt werden. Obwohl es auch zahlreiche Unterschiede gibt, die es Analysten ermöglichen, bestimmte Ransomware-Stämme bestimmten Familien oder Gattungen zuzuordnen, kann die Erkennung der Gemeinsamkeiten Sicherheitsteams dabei unterstützen, mehreren Varianten und Kampagnen entgegenzuwirken ohne jeden neuen Indikator kennen zu müssen. Zu den häufigsten Prozessen und Verhaltensmustern, die wir bei mehreren Ransomware-Stämmen erkennen konnten, zählen die folgenden:

1. Die Ransomware erstellt eine Anweisungsdatei auf dem Desktop: *readme.txt (MITRE: **T1105 Remote File Copy**)
2. Die Ransomware erzeugt eine cmd-Datei und stoppt Windows-Dienste und die AV-Software: cmd.exe /c sc.exe stop AVP /y (or stop*/y) (MITRE: **T1059 Command-Line Interface**, **T1089 Disabling Security Tools**)
3. Die Ransomware erzeugt eine cmd-Datei und löscht Schattenkopien: vssadmin.exe Delete Shadows /All /Quiet (Hinweis: "Delete Shadows" kann auch durch "shadowcopy delete" ersetzt werden) (MITRE: **T1059 Command-Line Interface**, **T1490 Inhibit System Recovery**)
4. Die Ransomware erzeugt eine cmd-Datei und verhindert eine Wiederherstellung: Bcdedit.exe /set {default} recoveryenabled no (MITRE: **T1059 Befehlszeilenschnittstelle**, **T1490 Inhibit System Recovery**)
5. Die Ransomware erzeugt eine cmd-Datei und verhindert eine Wiederherstellung: Bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures (MITRE: **T1059 Command-Line Interface**, **T1490 Inhibit System Recovery**)

Neben dem standardmäßigen Schwachstellen-Management, dem Patch-Management, der Erkennung und Abwehr von Malware und Bedrohungen, die auf heuristischen Mustern oder neuen Technologien basieren, kann sich auch die Deception-Technologie als geeignet erweisen, um maximalen Schutz zu gewährleisten.

Alt, aber immer noch bewährt

Wie bereits in einem anderen **Blog-Beitrag** beschrieben, geht das Threat Research Team von Fidelis davon aus, dass Cyberkriminelle mit ihrer Commodity-Malware auch weiterhin ältere Schwachstellen in etablierten Softwarelösungen und Diensten wie dem Internet Explorer, Oracle WebLogic und Adobe Shockwave/Flash nutzen werden. Neben Exploit-Kits setzen Cyberkriminelle auch häufig verschiedene Open-Source- und kommerzielle Tools ein, die für Penetrationstests und Forschungszwecke zur Verfügung stehen, um IT-Umgebungen und Netzwerke anzugreifen, in denen möglicherweise veraltete und anfällige Software und Lösungen genutzt werden. Dieser Trend wird vermutlich anhalten. Unternehmen sollten deshalb sicherstellen, dass sie die aktuellsten Versionen von Programmen einsetzen oder – wann immer möglich – bestimmte Software und Dienste deaktivieren und nicht länger bereitstellen.

Einschätzung des Threat Research Team von Fidelis

Die große Gefahr: Die Ausnutzung neuer Schwachstellen über Remote-Netzwerkdienste könnte Ransomware-Infektionen ähnlich wie bei WannaCry oder NotPetya auslösen. So könnten kriminelle, staatlich oder anderweitig organisierte Gruppierungen, die mit ausreichenden finanziellen Mitteln ausgestattet sind, Ransomware nutzen und Advanced Persistent Threats (APTs), Spionage-Aktionen oder Datendiebstahl im großen Stil umsetzen. Dies könnte schwerwiegende Probleme für Unternehmen und staatliche Organisationen nach sich ziehen und kritische Infrastrukturen wie das Finanzwesen, die Infrastruktur und die Versorgungseinrichtungen sowie die Verteidigung des Landes in Gefahr bringen.

Der Trend: Neue und bestehende Ransomware-Stämme werden weiterhin intensiv von gängigen Exploit-Kits eingesetzt und für die Ausnutzung älterer, bereits bekannter Schwachstellen genutzt. Da manche gängige Softwarelösungen wie Adobe Flash und der Internet Explorer auslaufen oder an Beliebtheit und Marktanteil verlieren, werden Exploit-Kits und Drive-by-Kampagnen weiterentwickelt, um sich an diese Veränderungen anzupassen und Ransomware sowie andere Payloads bereitzustellen. Dennoch werden Cyberkriminelle weiterhin versuchen, Schwachstellen in langjährig eingesetzten Softwarelösungen und Diensten auszunutzen, da veraltete Versionen dieser Lösungen immer noch genutzt werden und sie immer noch häufig genug erfolgreich damit sind.

Quellen:

- https://www.bleepingcomputer.com/news/security/new-lord-exploit-kit-pushes-njrat-and-eris-ransomware/
- https://bleepingcomputer.com/news/security/sodinokibi-ransomware-now-pushed-by-exploit-kits-and-malvertising/
- https://blog.malwarebytes.com/threat-analysis/2019/07/exploit-kits-summer-2019-review/
- https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread
- https://www.baltimoresun.com/politics/bs-md-ci-ransomware-attack-20190517-story.html
- https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/
- https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=210
- https://twitter.com/adrian__luca/status/1156934215566536705
- https://twitter.com/demonslay335/status/1133531771361005570
- https://twitter.com/nao_sec/status/1147831061004423168