Bitdefender

Sicherheit

Rekonstruktion eines chinesischen APT-Angriffs auf Regierungsbehörden in Südostasien

EXECUTIVE SUMMARY

Bitdefender-Sicherheitsforscher überwachen fortlaufend verschiedene APT-Gruppen und ihr Aktivitäten in aller Welt, um so ihre Taktiken, Vorgehensweisen und ihre bevorzugten Opfergruppen besser zu verstehen. Während es manchen APT-Gruppen ausschließlich um den finanziellen Profit geht, operieren andere auch im Auftrag von Regierungen und verfolgen auch politische Ziele. Forensische Artefakte, die von APT-Gruppen beim Einsatz eigens entwickelter Tools oder spezifischer Schadroutinen zurückgelassen werden, können nicht nur Hinweise auf bekannte Akteure liefern, sondern auch darauf, wie die Gruppen nach der Kompromittierung eines Ziels vorgehen. Im Rahmen der Überwachung der Aktivitäten von APT-Gruppen im asiatischen Raum fanden die Bitdefender-Forscher Anzeichen für einen komplexen und gezielten Spionageangriff, der sich gegen Regierungsbehörden in Südostasien richtete und der, ausgehend von den zurückgelassenen forensischen Artefakten, auf ein erfahrene chinesische APT-Gruppe zurückzuführen war. Die Operation erstreckte sich über mindestens einige Jahre, da die frühesten Anzeichen einer möglichen Kompromittierung auf Ende 2018 zurückgehen. Obwohl forensische Beweise eine Nachverfolgung des Angriffs bis ins Jahr 2020 hinein ermöglichen, wurden ein große Anzahl von C&C-Severn mittlerweile deaktiviert. Es ist davon auszugehen, dass die von der Gruppe kontrollierte und für den Angriff genutzte Infrastruktur derzeit inaktiv ist, auch wenn einige wenige C&Cs auch weiterhin funktionsfähig sind. Gegenstand dieser Untersuchung ist eine detaillierte Analyse des APT-Angriffs, um einen vollständigen Bericht über die eingesetzten Tools, Techniken und Verfahren zu liefern. Ziel von Bitdefender ist es, den zeitlichen Ablauf des Angriffs im Detail zu rekonstruieren, indem es alle forensischen Beweise in einer anschaulichen Fallstudie zusammenträgt. Darüber hinaus liefert der Bericht eine technische Analyse der Tools zur Durchführung dieses gezielten Angriffs und einen Überblick über das Zusammenspiel der einzelnen Komponenten. Der Angriff verfügt über ein komplexes und ausgedehntes Arsenal aus Droppern, Hintertüren und weitere Tools im Zusammenhang mit Chinoxy Backdoor, PCShare RAT und FunnyDream Backdoor-Binärdateien. Alle gefundenen forensischen Artefakte deuten dabei auf einen chinesischen Bedrohungsakteur mit umfassenden technischen Kenntnissen hin. Einige dieser Open-Source-RATs (Remote-Access-Trojaner) sind bekanntermaßen chinesischen Ursprungs. Darüber hinaus wurden weitere Ressourcen gefunden, die auf Chinesisch gestellt waren. Die Vielzahl von Persistenzmechanismen und Droppern, die die FunnyDream-Backdoor weitaus komplexer als die anderen eingesetzten Hintertüren machen, lassen darauf schließen, dass es sich um eine Eigenentwicklung handelt. Die frühesten Anzeichen des Angriffs gehen auf den November 2018 zurück, gefolgt von einer Zunahme der Aktivitäten der chinesischen APT-Gruppe ab Anfang 2019. Ab diesem Zeitpunkt und über einen Zeitraum von insgesamt fünf Monaten zeigten etwa 200 Systeme Anzeichen für die Einschleusung von verschiedenen Tools, die im Zusammenhang mit dem untersuchten APT-Angriff stehen. Dabei deuten einige Hinweise darauf hin, dass es Bedrohungsakteuren gelungen sein könnte, Domänencontroller im Netzwerk des Opfers zu kompromittieren, so dass sie sich in der Folge seitlich bewegen und möglicherweise die Kontrolle über eine große Anzahl von Rechnern in dieser Infrastruktur erlangen konnten. Die Untersuchung lässt auf einen Angriff schließen, dessen Ziel es war, Persistenz im Netzwerk herzustellen. Die Angreifer wollten möglichst lange unentdeckt bleiben, um ihr Opfer durch die Überwachung von Aktivitäten und die Exfiltration von Daten auszuspionieren.

ANGRIFFSÜBER-SICHT

Entdeckung einer potenziellen chinesischen APT-Gruppe, die mit einer komplexen Angriffsinfrastruktur, die auch heute noch teilweise einsatzbereit ist, gegen Regierungen in Südostasien vorgeht.

Bitdefender rekonstruiert erstmals den zeitlichen Angriffsablauf sowie die von der APT-Gruppe eingesetzten Tools, Techniken & Verfahren.

Vermutete Ziele

- Nationale Sicherheitsinteressen
- Industriespionage
- Ausschleusen sensibler Daten

Zielauswahl

- Hauptsächlich Regierungsbehörden in Südostasien

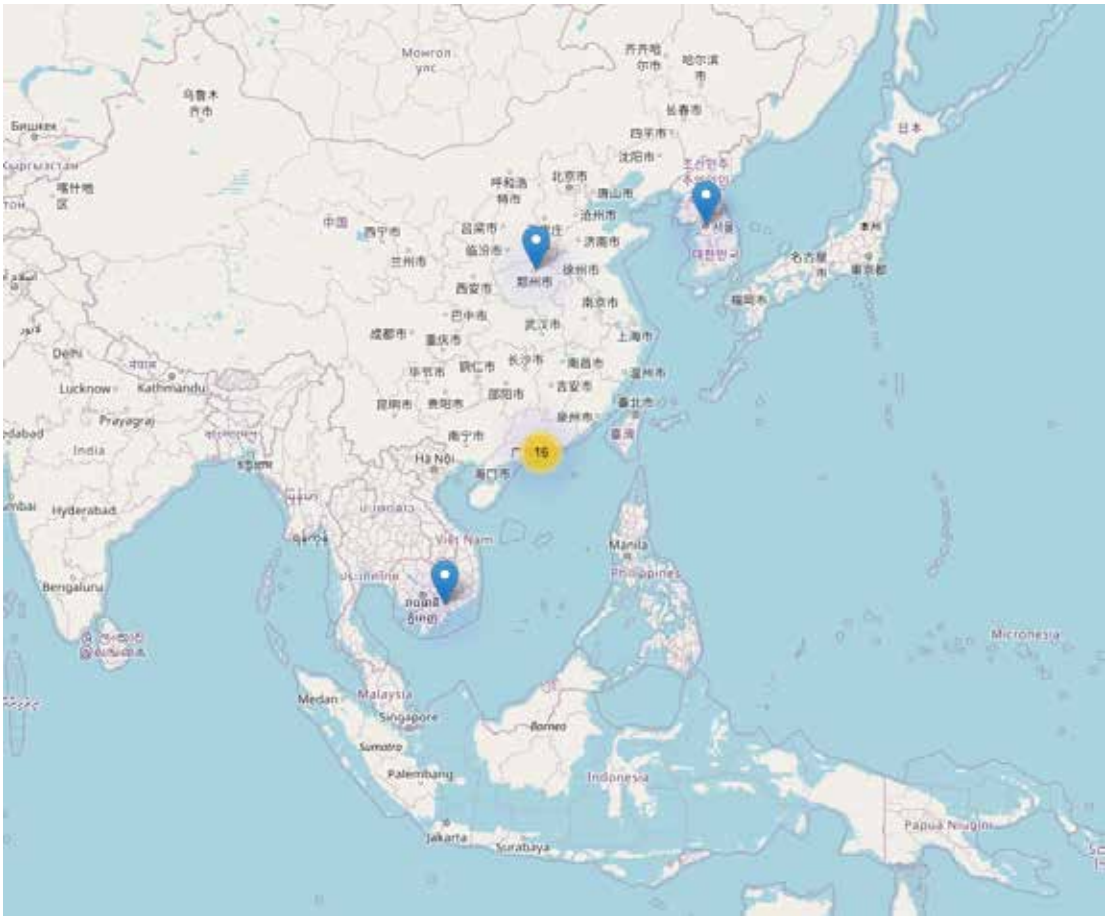
Exploit-Tools und -Verfahren

- Persistenz hergestellt durch digital signierte Binärdateien, die anfällig für das Einschleusen von Backdoors sind
- Umfangreiches, eigenentwickeltes Toolset für die Datenexploration und -exfiltration
- Drei Backdoors für das C&C: Chinoxy, PCShare, FunnyDream
- Potentiell kompromittierte Domänencontroller, die dem Angreifer Kontrolle über das Netzwerk des Opfers verschafften

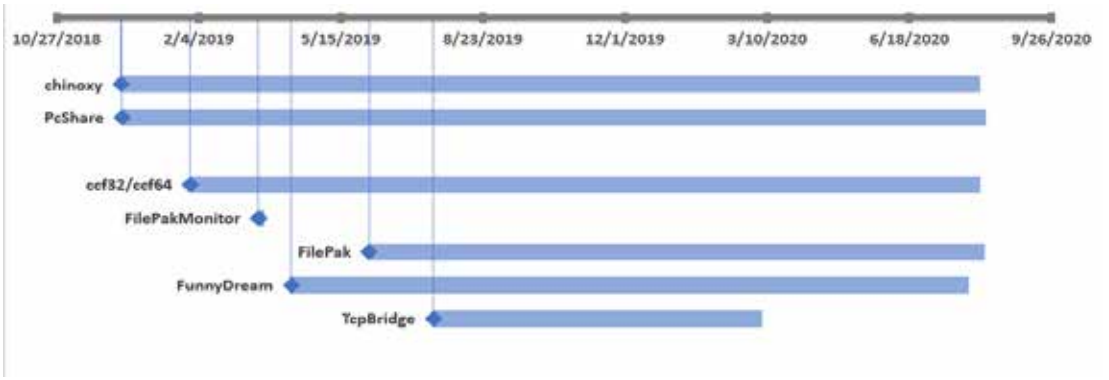
Reichweite der APT-Kampagne

- Artefakte nachweisbar von Ende 2018 bis hinein ins Jahr 2020
- Über 200 Computer mit Angriffsindikatoren im Zusammenhang mit der APT-Kampagne
- Angriffsinfrastruktur vermutlich auch heute noch aktiv

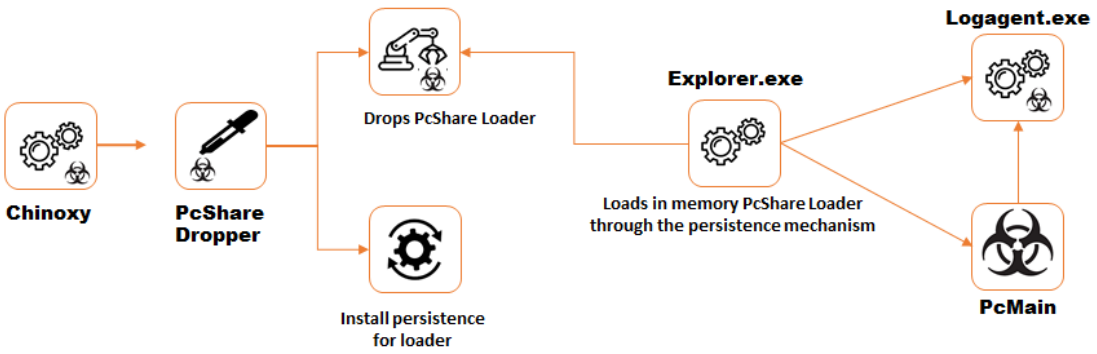
Standorte der APT-Command-and-Control-Infrastruktur



Zeitachse für den Einsatz des APT-Toolkits



Installation von PcMain, der primären Schadroutine des PCShare Remote-Access-Trojaners



Warum Bitdefender

Stolz im Dienste unserer Kunden

Bitdefender bietet Lösungen und Services für kleine und mittlere Unternehmen sowie Dienstleister und Firmen im Bereich Technologieintegration. Wir sind stolz auf das Vertrauen, das uns Unternehmen wie **Mentor, Honeywell, Yamaha, Speedway, Esurance oder Safe Systems** entgegenbringen.

Sieger im ersten Forrester Wave™-Report zur Sicherheit von Cloud-Workloads
Bewertung „empfehlenswert" beim NSS Labs AEP Group Test von NSS Labs
Zwei Jahre in Folge Auszeichnung zum SC Media Industry Innovator für die Hypervisor Introspection
Bewertung als „Representative Vendor of Cloud-Workload Protection Platforms" durch Gartner®

Ein Wort an unsere mehr als 20.000 Partner weltweit

Als exklusiver Channel-Anbieter verdankt Bitdefender seinen Erfolg auch seinem Netzwerk aus Wiederverkäufern und Vertriebspartnern.

Vier Jahre in Folge 5-Sterne-Partner von CRN Aufnahme in die „Security 100 List" von CRN
Zwei Jahre in Folge Cloud-Partner von CRN
Mehr MSP-Lösungen als jeder andere Sicherheitsanbieter
3 Bitdefender-Partnerprogramme, damit alle unsere Partner – Wiederverkäufer, Dienstleister und Hybridpartner – im Rahmen ihrer eigenen Spezialisierung sich vorrangig dem Vertrieb von Bitdefender-Lösungen widmen können

Vertrauenswürdige Sicherheitsinstitution

Bitdefender ist stolz auf seine Partnerschaften mit namhaften Virtualisierungsanbietern und den Beitrag, den wir gemeinsam mit **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS und Pivotal zur Entwicklung sicherer Ökosysteme leisten.**
Bitdefender ist zudem in enger Zusammenarbeit mit dem FBI und Europol aktiv an der Bekämpfung der internationalen Cyberkriminalität beteiligt und unterstützt Initiativen wie NoMoreRansom und TechAccord. So konnte Bitdefender z. B. zur Abschaltung des Online-Schwarzmarktes Hansa beitragen. 2019 wurde Bitdefender darüber hinaus von MITRE als CVE Numbering Authority autorisiert.

ANERKANNT VON FÜHRENDEN ANALYSTEN UND UNABHÄNGIGEN PRÜFORGANISATIONEN

TECHNOLOGIEPARTNERSCHAFTEN

Bitdefender®

Gründung 2001 in Rumänien
Anzahl der Mitarbeiter 1800+

Hauptsitz
Unternehmenszentrale – Santa Clara, Kalifornien, USA
Technologiezentrum – Bukarest, Rumänien

NIEDERLASSUNGEN AUF DER GANZEN WELT
USA & Kanada: Ft. Lauderdale, Florida | Santa Clara, Kalifornien | San Antonio, Texas | Toronto, Kanada
Europa: Kopenhagen, DÄNEMARK | Paris, FRANKREICH | München, DEUTSCHLAND | Mailand, ITALIEN | Bukarest, Iasi, Cluj, Timisoara, RUMÄNIEN | Barcelona, SPANIEN | Dubai, VAE| London, GB | Den Haag, NIEDERLANDE
Australien: Sydney, Melbourne

IM ZEICHEN DES WOLFS

Die Herausforderung des Fachgebietes Datensicherheit liegt darin, dass nur der klarste Blick, der schärfste Verstand und der tiefste Einblick gewinnen kann - Fehler sind keine Option. Unsere Aufgabe ist es, jedes Mal zu gewinnen, tausendmal aus 1.000 und 1 Million mal aus 1.000.000.

Und das tun wir. Wir sind der Leader in der Branche, jedem Hacker und Sicherheitsexperten um Schritte voraus. Der Scharfsinn unseres kollektiven Bewusstseins wird durch einen **hellleuchtenden Drachen-Wolf** repräsentiert. Er steht Ihnen zur Seite und schützt Sie mit seiner aus unserer Ingenieurskunst hervorgegangen Intuition vor allen Gefahren, die in den verborgenen Tiefen der digitalen Welt lauern.

Dieser Scharfsinn ist unsere Superkraft und bildet den Kern all unserer richtungsweisenden Produkte und Lösungen.

Bitdefender-ESDC-APTDS-creat1492f-de_DE
1/16/20November 16, 2020 9:21 pm 1/16/20