SUPPLY CHAIN COMPROMISES

UNDERSTAND THE THREAT & DEFEND YOUR ORGANISATION

AARON AUBREY NG

CROWDSTRIKE

AARON AUBREY NG

STRATEGIC THREAT ADVISOR, APJ & MENA

ARMY | GOVERNMENT | INTELLIGENCE | INDUSTRY

- **10+ years:** Innovating at the intersection of Intelligence, Security, and Strategy
- **Government**: Former Intelligence Officer/Major in the Singapore Armed Forces; Served in the Military Intelligence Organisation (MIO) and the Defence Cyber Organisation (DCO)
- **Private Sector**: Designed and built threat intelligence programs for large Fortune 500 companies and government agencies across APJ
- **Education**: MSc Management Science & Engineering from Stanford University; BEng Chemical Engineering from University College London
- **Professional Accreditations**: GCTI | GPEN | GCIA | GOSI | GCIH | GSEC

aaron(dot)ng@crowdstrike.com

+65 9856 8896

Aaron Aubrey Ng @ CrowdStrike

ALL CONTENT CONTAINED WITHIN THIS INTELLIGENCE BRIEF WAS DERIVED FROM CROWDSTRIKE INTELLIGENCE REPORTING AND PUBLIC SOURCES

NO CONTENT WITHIN THIS BRIEF WAS DERIVED FROM CROWDSTRIKE INCIDENT RESPONSE ENGAGEMENTS

CROWDSTRIKE IS UNABLE TO ANSWER QUESTIONS PERTAINING TO CROWDSTRIKE INCIDENT RESPONSE ENGAGEMENTS

CROWDSTRIKE

AGENDA

OVERVIEW OF SUPPLY CHAIN COMPROMISE

STELLARPARTICLE ACTIVITY CLUSTER

SUPPLY CHAIN ATTACK VECTORS

WHAT NEXT?

CROWDSTRIKE

SUPPLY CHAIN COMPROMISE

UPSTREAM TRUST

LONG TIME HORIZONS

CLANDESTINE ACCESS

CROWDSTRIKE

WHY IS IT SO DIFFICULT TO DETECT SUPPLY CHAIN ATTACKS?

ADVERSARY

PHISHING

EMAIL GATEWAY

VICTIM

CROWDSTRIKE

WHY IS IT SO DIFFICULT TO DETECT SUPPLY CHAIN ATTACKS?

ADVERSARY

PORT SCAN

EMAIL GATEWAY

FIREWALL SETTINGS

VICTIM

CROWDSTRIKE

WHY IS IT SO DIFFICULT TO DETECT SUPPLY CHAIN ATTACKS?

ADVERSARY

BANKING TROJAN

EMAIL GATEWAY

FIREWALL SETTINGS

AV/EDR SENSOR

VICTIM

CROWDSTRIKE

WHY IS IT SO DIFFICULT TO DETECT SUPPLY CHAIN ATTACKS?

ADVERSARY

SUPPLY CHAIN ATTACK

THIRD-PARTY PROVIDER

EMAIL GATEWAY

FIREWALL SETTINGS

AV/EDR SENSOR

NO PERFECT ANSWER

VICTIM

CROWDSTRIKE

WHY IS IT SO DIFFICULT TO DETECT SUPPLY CHAIN ATTACKS?

THIRD-PARTY PROVIDER

EMAIL GATEWAY | FIREWALL SETTINGS | AV/EDR SENSOR | NO PERFECT ANSWER

ADVERSARY

SUPPLY CHAIN ATTACK

1:MANY – ATTACK ONCE, AFFECT COUNTLESS VICTIMS

VICTIM A | VICTIM B | VICTIM C | VICTIM D

CROWDSTRIKE

WHY IS IT SO DIFFICULT TO DETECT SUPPLY CHAIN ATTACKS?

THIRD-PARTY PROVIDER

EMAIL GATEWAY | FIREWALL SETTINGS | AV/EDR SENSOR | NO PERFECT ANSWER

ADVERSARY

1:MANY – ATTACK ONCE, AFFECT COUNTLESS VICTIMS

VICTIM A | VICTIM B | VICTIM C | VICTIM D


SUPPLY CHAIN COMPROMISES

EVOLUTION OF SUPPLY CHAIN COMPROMISES

EARLY 2000s - ONGOING

HISTORICALLY TARGETED COMMONLY KNOWN VULNERABILITIES THAT WERE LEFT ***UNPATCHED*** BY ORGANIZATIONS

INSTEAD OF WAITING FOR PUBLIC VULNEREABILITY DISCLOSURES, ADVERSARIES ***PROACTIVELY*** INJECT MALICIOUS CODE INTO PRODUCTS

IMPACTED PRODUCTS ARE LEGITIMATELY DISTRIBUTED THROUGH GLOBAL SUPPLY CHAIN > PERTINENT FOR ***COMMERCIAL*** & ***OPEN SOURCE*** PRODUCTS

STELLARPARTICLE

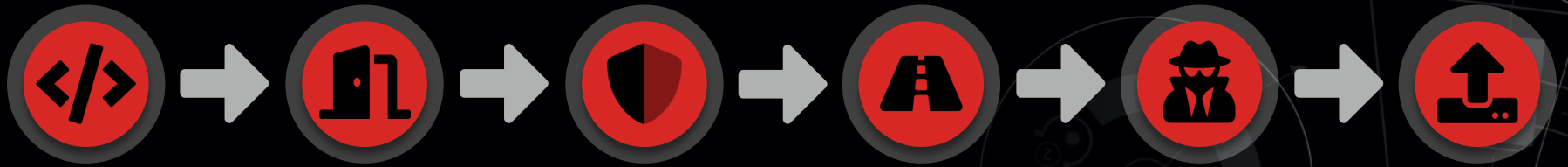
ACTIVITY CLUSTER

INCIDENT HIGHLIGHT: SOLARWINDS ATTACK

- 13 DEC 2020 - PUBLIC REPORTS OF A SOPHISTICATED SUPPLY CHAIN ATTACK AGAINST SOLARWINDS
- MALICIOUS CODE OBSERVED ON LARGE NUMBER OF ORGS (~18K) ACROSS MULTIPLE VERTICALS
- ENABLED ACCESS TO US TREASURY & COMMERCE DEPTS, NATIONAL TELCO & INFO ADMINSTRATION (NTIA)
- INDICATIVE OF A SOPHISTICATED ADVERSARY WITH CUSTOM TOOLING AND ADVANCED TTPS

CROWDSTRIKE

STELLARPARTICLE KILL CHAIN



BUILD ENVIRONMENT COMPROMISE

SUNSPOT EXPLOITS BUILD ENVIRONMENT THROUGH SOURCE CODE REPLACEMENT

INITIAL ACCESS

SUNBURST BACKDOOR INSTALLED VIA COMPROMISED SOFTWARE UPDATE

DEFENSE EVASION

- STRING OBFUSCATION
- DISABLE SECURITY PRODUCTS ON RESTART
- EXECUTION GUARDRAILS
- MASQUERADES C2 TRAFFIC

LATERAL MOVEMENT

TEARDROP AND RAINDROP DEPLOYED
→ COBALT STRIKE

LONG-TERM PERSISTENCE

- GOLDMAX TO MAINTAIN ACCESS TO BREACHED ENVIRONMENT
- GOLDFINDER FOR ADDITIONAL RECON BEFORE DEPLOYING GOLDMAX

DATA EXFILTRATION

HTTP-BASED C2

COZY BEAR

DYNAMIC & WELL-RESOURCED ADVERSARY

2011 - ONGOING

- TARGETING SCOPE ALIGNED WITH ***POLITICAL ESPIONAGE***
- ASSESSED TO BE ACTING ON BEHALF OF THE RUSSIAN ***FOREIGN INTELLIGENCE*** SERVICE (SVR / СВР РФ)
- DEMONSTRATES ***PERSISTENCE*** AND FOCUS ON SPECIFIC TARGETS, INCLUDES ***GOVT/POLITICAL*** ORGS AND NGOS
- UNDERTAKES LARGE VOLUME ***SPEAR-PHISHING*** CAMPAIGNS TO DELIVER EXTENSIVE RANGE OF MALWARE
- SOPHISTISCATED TOOLS IMPLEMENTED WITH EXTENSIVE ***CRYPTOGRAPHY*** AND ***ANTI-ANALYSIS*** TECHNIQUES

SUPPLY CHAIN

ATTACK VECTORS

CROWDSTRIKE

SUPPLY CHAIN ATTACK VECTORS

SOFTWARE

HARDWARE

TRUSTED RELATIONSHIP


CROWDSTRIKE
SOFTWARE
SUPPLY CHAIN
THREATS

CROWDSTRIKE

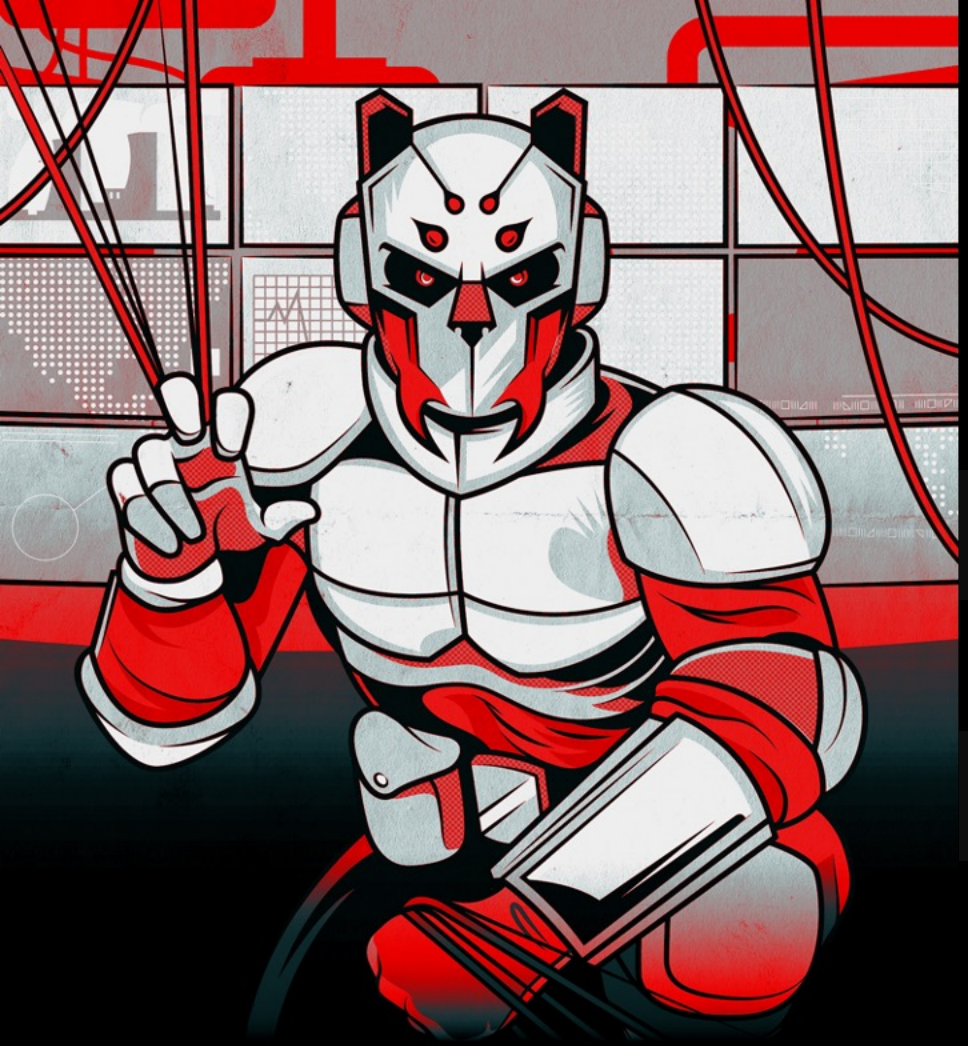
METHODS OF COMPROMISE – SOFTWARE SUPPLY CHAIN

SOFTWARE
DESIGN FLAWS

VULNERABLE
3P COMPONENT

INFILTRATE
SUPPLIER NETWORK

INJECT
MALICIOUS CODE



WICKED PANDA

PROLIFIC & ENDURING ADVERSARY

2010s - ONGOING

- TARGETING SCOPE ALIGNED WITH CCP OBJECTIVES IN 13th & 14th FIVE YEAR PLANS AND MADE IN CHINA 2025
- CONTRACTORS WORKING FOR THE MSS WHILE PERFORMING CRIMINAL ACTIVITIES WITH TACIT APPROVAL
- HISTORY OF SOFTWARE SUPPLY CHAIN COMPROMISES FOR FINANCIAL GAIN AND ESPIONAGE PURPOSES
- KNOWN FOR RAPID IDENTIFICATION AND EFFECTIVE EXPLOITATION OF NOVEL VULNERABILITIES > ***LOG4J***
- RELIES HEAVILY ON ***COBALT STRIKE*** AND HAS BEEN DELIVERING ***ATTACHLOADER***, ***PLUGX***, ***WINNTI*** TO TARGETS

WICKED PANDA

PROLIFIC TRACK RECORD OF SUPPLY CHAIN COMPROMISES

DEC '14	SOUTHEAST ASIAN VIDEO GAME DISTRIBUTOR
MAR '17	CCLEANER UTILITY
JUL '17	NETSARANG SOFTWARE PACKAGES
JUN – NOV '18	ASUS LIVE UPDATE UTILITY / SHADOWHAMMER
JUL '18	SOUTHEAST ASIAN VIDEO GAME DISTRIBUTOR

IN 2019 – 2020, **FOUR** EXAMPLES OF SUPPLY CHAIN COMPROMISES IN SOFTWARE **REQUIRED** BY CHINESE GOV AUTHORITIES > EMPLOYED FOR **SURVELLIANCE**?

LOG4J/LOG4SHEL
SETS THE INTERNET ON FIRE

EXPLOITATION OF UBIQUITOUS LOGGING LIBRARY

VULN REPORTED IN NOV 21 - ***CVE-2021-44228*** / ***LOG4SHELL*** > INJECT JAVA CODE INTO AFFECTED SVCS

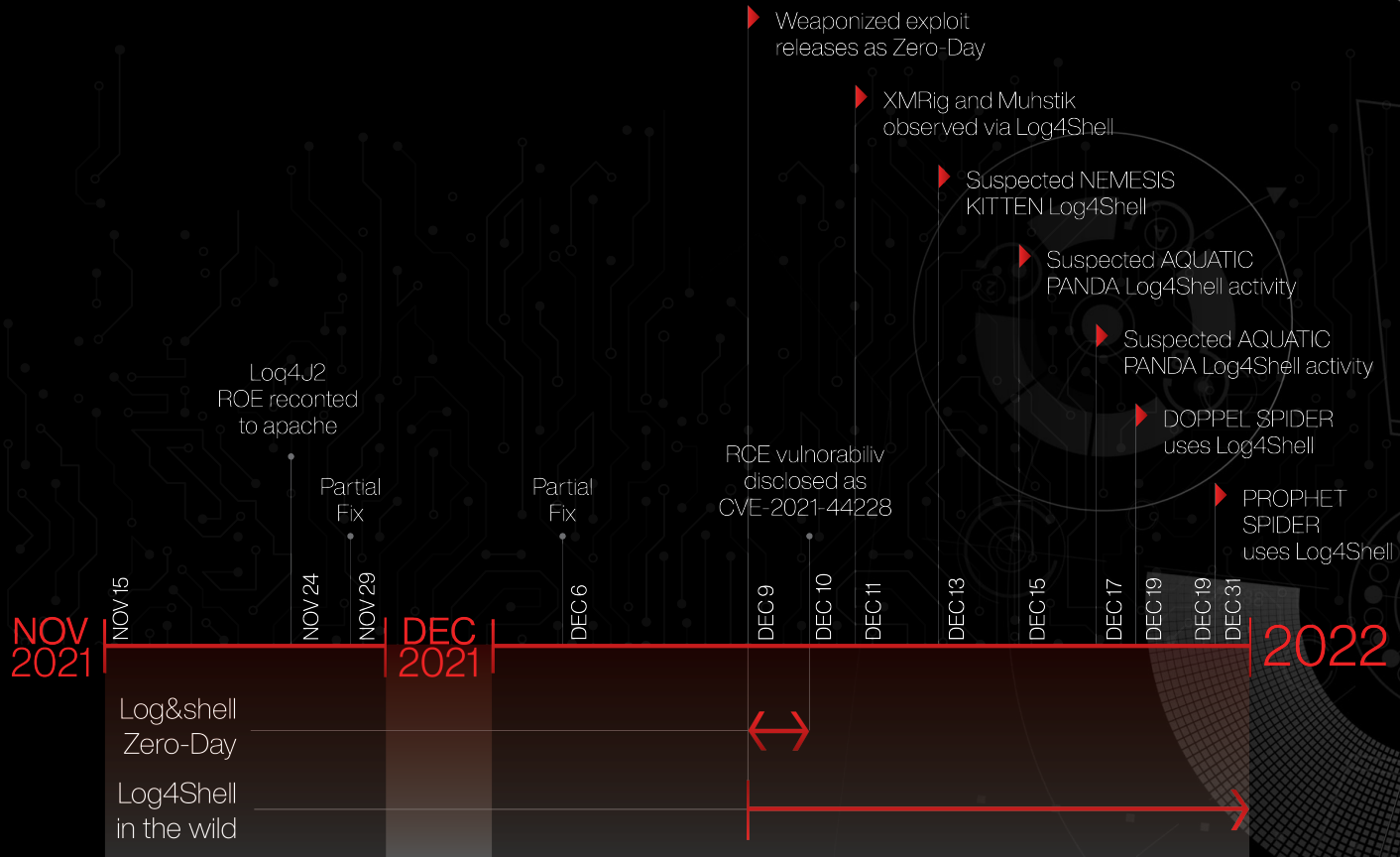
SPECIFICALLY CRATED REQUESTS RESULT IN ***ACCESS*** TO SYSTEM, DELIVER ***MALWARE***, ACQUIRE ***DATA***/***CREDS***

ECRIME ADVERSARIES AGGRESSIVELY ENGAGED IN WIDESPREAD EXPLOITATION > ***BOTNET*** MALWARE

STATE-NEXUS ACTORS – ***NEMESIS KITTEN*** & ***AQUATIC PANDA*** OBSERVED LOG4SHELL EXPLOITATION ACTIVITY

CROWDSTRIKE

TIMELINE OF LOG4SHELL EVENTS



AQUATIC PANDA

PROLIFIC DUAL-MISSION ADVERSARY

INTELLIGENCE COLLECTION & INDUSTRIAL ESPIONAGE

- ACTIVE SINCE MAY 2020 – TARGETS TELCO, TECH, ACADEMIA, GOVT, MILITARY SECTORS ACROSS ASIA
- PROLIFIC ADVERSARY – TARGETED ***~100 ORGS*** IN 17 COUNTRIES OVER 2021
- HISTORY OF TARGETING ***GOVT***, ***MILITARY***, ***TECH***, ***RESEARCH*** ENTITIES ACROSS SOUTHEAST ASIA
- RELIES HEAVILY ON ***COBALT STRIKE*** AND HAS BEEN DELIVERING ***NJRAT***, ***SHADOWPAD***, WINNTI TO TARGETS
- ASSESSED TO BE ***CONTRACTOR*** SERVING THE ***MSS*** WITH INTEL FOR GEOPOL AND ECONOMIC DEVMT


CROWDSTRIKE
HARDWARE
SUPPLY CHAIN
THREATS

CROWDSTRIKE

HARDWARE SUPPLY CHAIN ATTACKS

TAMPERING

HARDWARE MODIFICATIONS MADE TO ASSETS DURING MANUFACTURING

COUNTERFEIT

REPLACING LEGITIMATE PRODUCTS WITH COUNTERFEIT VERSIONS


CROWDSTRIKE
TRUSTED
RELATIONSHIP
THREATS

OPERATION CLOUD HOPPER
THIRD-PARTY COMPROMISE

MULTI-YEAR CYBER ESPIONAGE CAMPAIGN

STONE PANDA TARGETED MANAGED IT SERVICE PROVIDERS IN NORTH AMERICA, EUROPE, SOUTH ASIA

EXPLOITED TRUSTED ACESS TO STEAL INFORMATION FROM MSP CUSTOMERS

VICTIMS INCLUDE – HPE, IBM, FUJITSU, TCS, NTT DATA, DIMENSION DATA, AND DXC TECH

LARGE QUANTITIES OF ***INTELLECTUAL PROPERTY*** STOLEN FROM GLOBAL COMPANIES AND GOVT ORGS

INCIDENT HIGHLIGHT: KASEYA RANSOMWARE ATTACK

- 2 JULY 2021 - RANSOMWARE ATTACK AFFECTING ORGANIZATIONS USING KASEYA VSA
- PINCHY SPIDER'S REVIL DETERMINED TO BE VARIANT USED IN THE ATTACK
- TARGETING SERVICE PROVIDERS TO SCALE RANSOMWARE DISTRIBUTION
- RANSOM DEMAND APPROXIMATELY $70M

PINCHY SPIDER

BIG GAME HUNTING RANSOMWARE

2018 - ONGOING

- CRIMINAL GROUP BEHIND THE DEVELOPMENT AND OPERATION OF ***REVIL*** (***SODINOKIBI***) RANSOMWARE
- AT THE GROUP'S PEAK, REVIL WAS ONE OF THE MOST PROLIFIC ***RANSOMWARE-AS-A-SERVICE*** PROGRAMS
- HISTORY OF ***OPPORTUNISTIC*** TARGETING > GEOGRAPHICALLY AND SECTOR AGNOSTIC
- LATE 2021 – SUBJECTED TO SERIES OF US LAW ENFORCEMENT ACTION DIRECTED AT THE GROUP
- MAY 2022 – ***NEW SAMPLES*** OF REVIL COMPILED BY SOMEONE WITH FULL ACCESS TO SOURCE CODE

WHAT

NEXT?

WHITHER SUPPLY CHAIN COMPROMISES?

RAPID VULN EXPLOITATION

GEO DISPERSED SUPPLY CHAIN

OPEN SOURCE PROLIFERATION

CLOUD & CONTAINERS

CROWDSTRIKE

STRIVING TOWARDS SUPPLY CHAIN SECURITY

RISK MANAGEMENT

ADOPT SUPPLY CHAIN RISK MANAGEMENT

SECURE DEVELOPMENT

IMPLEMENT SECURE SDLC PROCESSES & PRACTICES

VERIFY 3P COMPONENTS

TRUSTED SUPPLIER REVIEW & TEST SOFTWARE BOM

CLOUD SECURITY

VISIBILITY & PROTECTION FOR CLOUD ASSETS

THREAT INTELLIGENCE

ADVERSARIES
VULN INTELLIGENCE
THIRD PARTY RISK

CROWDSTRIKE