Hacker-Lexikon: Was sind CNE und CNA?

Autor: Kim Zetter.Kim Zetter Sicherheit

WIRED | 2016.07.06

Seit Jahren ist die US-Offensive Hacking Operationen der Regierung wurden in dunklen Schatten gehalten, weder anerkannt noch diskutiert. Das änderte sich mit der Entdeckung von Stuxnet in 2010-Sabotage Betrieb Computer angeblich von den USA und Israel durchgeführt Maschinen im Iran einst illegalen Nuklearprogramm verwendet zu zerstören.

Stuxnet war der erste US-digitale Sabotage Betrieb ausgesetzt werden, aber es ist nicht die erste Regierung Hacking Operation jemals durchgeführt wurde. Dokumente sickerte durch Edward Snowden im Jahr 2013 leuchtete ein Licht auf einem riesigen unterirdischen Betrieb durch den maßgeschneiderten Zugriffsoperationen Team der NSA durchgeführt (TAO), verantwortlich für das, was die Regierung bezieht sich auf als Computer-Netzwerk-Nutzung und Computer-Netzwerk-Attacken. Diese können ähnlich klingen, aber es gibt wichtige Unterschiede zwischen ihnen.

Computer-Netzwerk-Nutzung, oder CNE, bezieht sich auf Spionage und Aufklärung Operationen. Diese werden durchgeführt, Daten von einem System zu stehlen oder einfach Intelligenz über Netzwerke zu erhalten, zu verstehen, wie sie funktionieren und konfiguriert sind. Beispiele für CNE umfassen Flamme, eine massive Spion Werkzeug zu sammeln Intelligenz aus dem Iran und andere Ziele verwendet, und Regin, der verwendet wurde, die Europäische Kommission und die belgische teilweise staatlichen Telekom-Belgacom zu hacken. Die Regin Operationen wurden dem britischen Geheimdienst GCHQ zugeschrieben.

Ein Katalog von benutzerdefinierten NSA Hacker-Tools im Jahr 2013 zu den Reportern durchgesickert zeigt die enormen Fähigkeiten zur Verfügung zu TAO Hacker. Die Werkzeuge, mit Namen wie PICASSO, IRATEMONKEY, Cotton und WATERWITCH können Firewalls, Servern unterminieren und Router oder GSM-Basisstationen ausgeben Mobiltelefon Anrufe abfangen oder Daten von drahtlosen Netzwerken Siphon. Es gibt auch Geräte, die TAO-Hacker-Anlage in Zielcomputer nervt Daten abzuschöpfen, über Funkwellen, zu Hörstationen, manchmal liegt bis zu acht Meilen entfernt von einer Maschine des Opfers.

Im Jahr 2011 startete die NSA 231 Offensive Computer-Operationen, nach Snowden Dokumenten. Dazu gehörten Platzierung verdeckte Implantate in mehr als 80.000 Maschinen weltweit.

Wenn Sie von CNE als Oceans Elf von Cyber-Attacken zu denken, ist CNA mehr wie Die Hard.

CNA-Operationen sind so konzipiert, zu beschädigen, zu zerstören oder zu stören Computer-oder Computer-so gesteuert Operationen wie der Stuxnet-Angriff, Zentrifugen durch Iran verwendet gezielte Uranhexafluoridgas zu bereichern. Ein weiterer CNA Operation Nationalstaaten zurückzuführen ist die Luft-Boden-Hack Leitung von Israel im Jahr 2007 gegen die syrische Luftabwehrsystem. Das Hack, von israelischen Flugzeugen ins Leben gerufen, wurde entwickelt, Syriens automatisierte Flugabwehrsystem vom Sehen Bomber Jets fliegen in zu führen einen Luftangriff gegen die Al-Kibar-Komplex zu verhindern, vermutlich um einen illegalen Kernreaktor Syrien zu sein war der Bau.

Die jüngste Hack von Energieverteilungsanlagen in der Ukraine war ein CNA, da die Wischer Angriff war, dass der Iran die Ölindustrie im Jahr 2012 gezielt Dieser Angriff Daten von Maschinen gehören, zu dem iranischen Ölministerium und der National Iranian Oil Company gewischt. Der Hack von Sony, zurückzuführen auf Nordkorea, wäre auch ein CNA Betrieb angesehen werden, da die Hacker einfach

nicht Daten aus dem Netzwerk des Unternehmens Siphon, sie zerstört auch Daten und Systeme auf dem Weg aus der Tür.

Obwohl CNE und CNA-Operationen technisch distinct-da zu sein scheinen könnte ein Spionage und die andere Zerstörung oder beinhaltet störungs sie sind nicht unbedingt. Viele CNA Angriffe beginnen als CNE-Operationen, da Angriffen, oft verursachen Zerstörung digitale Aufklärung und Nachrichtengewinnung erfordern zuerst. Die Bande von Hackern, die Stuxnet ins Leben gerufen, zum Beispiel entwarf auch mehrere Spion Werkzeuge, von denen einige sind vermutlich verwendet wurden Erkenntnisse über den Computer zu gewinnen Kontrolle der iranischen Zentrifugen, die dann dazu verwendet wurde, den schädlichen Code zu entwerfen, die Zentrifugen zerstört.

Da einige Tools für beide CNE und CNA-Attacken, zum Beispiel Null Tage verwendet werden, verwendet werden, um beide Spionage-Tools zu installieren und Angriffs-Tools auf gezielte system kann es für die Opfer schwierig sein, die eine solche Malware auf ihren Rechnern finden zu wissen, ob die Operation eine Spionagemission oder ein Angriff Mission; zumindest, das heißt, bis ihre Systeme zerstört werden.

Zurück zum Anfang. Wechseln zu: Anfang des Artikels.

lesen: https: //www.wired.com/2016/07/hacker-lexicon-cne-cna/