Oznámení o možné nákaze malware

Chtěli bychom Vás informovat jako osobu odpovědnou za informační bezpečnost o pravděpodobně infikovaných strojích ve Vaší kompetenci.

Důvodem proč Vás kontaktujeme je komunikace IP adres(y) se sinkhole serverem, který zaznamená přístup k C&C. Uvedené domény, které byly kontaktovány jsou/byly spojovány s botnetem Dorkbot. Proto vzniklo podezření na možnou infekci tímto malwarem.

DORKBOT

Stručná charakteristika

Patří do skupiny škodlivých kódů, které zprostředkují útočníkovi přístup a kontrolu nad napadeným strojem. Mezi základní funkce patří krádež hesel (Facebook, Twitter,…), sběr informací a distribuce dalšího malware na již kompromitovaném stroji.

Dorkbot se může šířit pomocí sociálních sítí, SPAMu, vyměnitelných médií a exploit kitů. Jakmile je nainstalován brání v činnosti bezpečnostnímu software, blokováním přístupu k aktualizacím. Zároveň se připojí na IRC server a očekává další instrukce. Jednou z hlavních schopností tohoto malware je distribuce dalšího malware na již nakažený stroj. Může se jednat o malware umožňující provádění DDoS útoků nebo rozesílání SPAMu

Varianty

Více informací o jednotlivých variantách tohoto botnetu naleznete na konci tohoto dokumentu.

Botnet

Základní struktura Botnetu se skládá ze dvou částí. Řídící servery (Command & Control) a koncové uzly.

Koncový uzel je zpravidla infikován nějakým druhem malwaru. Zároveň se snaží v pravidelných intervalech kontaktovat C&C server(y).

Botnet může sloužit k ro-zesílání SPAMu, rozšiřová-ní virů, DDoS útokům a jiným druhům počítačové kriminality.

Odstranění možné nákazy

Pro odstranění možné nákazy můžete použít například nástroj MSRT (Malicious Software Removal Tool), který je ke stažení zde: http://www.microsoft.com/security/pc-security/malware-families.aspx. Nástroj je dostupný na platformě Windows (Windows 2000, Windows XP, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008 a Windows Server 2012). Pomáhá odstranit malware a jiné nalezené infekce, jmenujme například: Bamital, Caphaw, Conficker, Kelihos, Nitol, Rustock, Simda, Waledac, Zbot a další. Eventuálně doporučujeme úplnou kontrolu stroje antivirovým SW s nejnovější virovou databází.

Prevence

Doporučujeme vždy aktualizovat operační systém, tj.: zapnutý Windows Update, personální firewall a také aktuální verzi antivirového software s aktuální virovou databází. Nezapomeňte také pravidelně aktualizovat veškerý software nainstalovaný na počítači.

Komunikace

V případě jakýchkoli otázek nebo nejasností nás neváhejte kontaktovat na adrese: cert.incident@nbu.cz. Zároveň bychom Vás chtěli požádat o informace – jak jste postupovali při identifikaci, odstranění a prevenci případné budoucí nákazy. Prosíme o zaslání informací i v případě, že uvedené stroje nebyly nákaze vystaveny.

Komentář k přiloženým souborům

Soubory jsou ve formátu CSV.

Soubor ip.csv obsahuje základní údaje pro každý infikovaný počítač a má následující strukturu:

Pole	Jméno	Popis
0	Id	Identifikátor
1	Ip_address	IP adresa
2	Threat	Jméno botnetu
3	Latitude	Zeměpisná šířka
4	Longtitude	Zeměpisná délka
5	Constituency	Organizace, pod kterou spadá IP
6	State	Označení státu
7	Whois name	Jméno uvedené v WHOIS DB
8	Whois descr	Popis uvedený v WHOIS DB

Soubor raw.csv obsahuje veškeré pokusy o připojení infikovaného počítače k C&C a má následující strukturu:

Pole	Jméno	Popis
0	Id	Identifikátor
1	SourcedFrom	Informace „SinkHole“
2	FileTimeUtc	Časová známka zprávy odpovídá lokální časové zóně
3	Botnet	Jméno botnetu
4	SourceIp	Zdrojová IP adresa
5	SourcePort	Zdrojový port
6	SourceIpAsnNr	Číslo ASN pod které spadá IP adresa
7	TargetIp	Cílová IP adresa
8	TargetPort	Cílový port
9	Payload	Obsah zprávy
10	SourceIpCountryCode	Označení státu
11	SourceIpRegion	Označení regionu
12	SourceIpCity	Označení města
13	SourceIpPostalCode	Směrovací číslo
14	SourceIpLatitude	Zeměpisná šířka
15	SourceIpLongitude	Zeměpisná délka
16	SourceIpMetroCode	Další informace o zdrojové IP
17	SourceIpAreaCode	Další informace o zdrojové IP
18	HttpRequest	Požadovaná HTTP adresa
19	HttpReferrer	HTTP hlavička
20	HttpUserAgent	Použitý prohlížeč
21	HttpMethod	HTTP metoda
22	HttpVersion	HTTP verze
23	HttpHost	HTTP host hlavička
24	Custom Field 1	R2: příkaz password, který předcházel druhému pakeku poslaným stejným klientem.
25	Custom Field 2	R2: msg v hex (max. 50 bytes)
26	Custom Field 3	R2S: tři pole (SSL session ID, velikost paketu 1, velikost paketu 2); R2V: dva pakety (velikost paketu 1, velikost paketu 2)
27	Custom Field 4	R1: heslo; R2: nickname
28	Custom Field 5	R1: msg v hex; R2: msg v hex
29	Threat Confidence	High / Medium / Low / Informational / None

Hodnota pole *Ip_address* odpovídá hodnotě v poli *SourceIp*. Stejně tak si odpovídají pole *Threat*.

Varianty malware Dorkbot

Označení	Popis
B85-R1V	Záchyt první zprávy – nešifrovaná komunikace. Čtyř písmena, zpravidla PASS následované mezerou a unikátním heslem botnetu.
B85-R1S	Záchyt první zprávy – šifrovaná komunikace. Čtyř písmena, zpravidla PASS následované mezerou a unikátním heslem botnetu.
B85-R2V	Záchyt druhé zprávy – nešifrovaná komunikace. Může obsahovat některé informace: a) nickname příkaz (NICK nebo KCIK nebo SSRR) např. NICK steve nebo KCIK joe b) identifikaci OS (např. XPa, W7a,…) c) unikátní 7 znakový řetězec generovaný infikovanou stanicí
B85-R2S	Záchyt druhé zprávy – šifrovaná komunikace. Může obsahovat některé informace: a) nickname příkaz (NICK nebo KCIK nebo SSRR) např. NICK steve nebo KCIK joe b) identifikaci OS (např. XPa, W7a,…) c) unikátní 7 znakový řetězec generovaný infikovanou stanicí