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 b75. Proto vzniklo podezření na možnou infekci tímto malwarem.

B75

Stručná charakteristika

Jedná se o modulární malware. Obsahuje moduly následující moduly, které umí unášet spojení k bankovním účtům a sociálním sítím, sbírá přihlašovací údaje z FTP klientů. Součástí je také modul umožňující vzdálený přístup k počítači (VNC), anonymní FTP. Špionážní modul umožňuje útočníkovi provést Man-in-the-browser útok za účelem získání citlivých informací.

Nejčastěji se tento malware šíří pomocí výměnných zařízení jako jsou USB klíčenky a sítové disky. Útočník může také použít FTP server, exploit kit s využitím infikované reklamy nebo je malware součástí potencionálně nechtěných aplikací, aby stroj nakazil.

Více informací o této hrozbě naleznete v dokumentu: W32.Ramnit analysis

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 rozesílání 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, Conficker, Kelihos, Nitol, Ramnit, Rustock, 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 verze 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

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	Threat	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	Unikátní ID pro infikovaný stroj
25	Custom field 3	6 B preambule/ 7 B paketu
26	Custom field 4	1 B příkazu

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

Varianty malware b75

Označení	Popis
B75-S1	**Stroj zaslal příkaz C&C serveru.**
B75-S12	**Stroj odeslal příkaz k autentizující se C&C serveru. První paket obsahuje preambuli. Druhý paket je potvrzujícím.**
B75-S2	**Stroj předal příkaz k autentizující se C&C serveru. V jednom paketu obsahuje preambuli i potvrzení.**