

## 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 b106. Proto vzniklo podezření na možnou infekci tímto malwarem.

### B106

#### Stručná charakteristika

Poznávacím znamením této skupiny malware je komunikace s dynamickými DNS službami. Nejčastěji se jedná o No-IP. Zaměření tohoto botnetu je získání uživatelských údajů a citlivých informací od uživatelů. Některé varianty mohou pořizovat snímky obrazovky nebo zaznamenávat video.

Nejčastěji se tento malware šíří pomocí sociálního inženýrství. Může se jednat o navštívení nakažených stránek nebo kliknutí na link směřující na infikované stránky. Jiné varianty se šíří pomocí torrentů nebo programů kde je malware jeho součástí. Vydává se například za Adobe Flash Player.

### Varianty

Pod souhrnným označením b106 vystupuje více než 35 různých hrozeb. Jedná se například o: Bladabindi, Injector nebo Jenxcus.

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 rozšíření SPAMu, rozšiřování 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, 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](mailto: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	Longitude	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	Sourcelp	Zdrojová IP adresa
5	SourcePort	Zdrojový port
6	SourcelpAsnNr	Číslo ASN pod které spadá IP adresa
7	TargetIp	Cílová IP adresa
8	TargetPort	Cílový port
9	Payload	Obsah zprávy
10	SourcelpCountryCode	Označení státu
11	SourcelpRegion	Označení regionu
12	SourcelpCity	Označení města
13	SourcelpPostalCode	Směrovací číslo
14	SourcelpLatitude	Zeměpisná šířka
15	SourcelpLongitude	Zeměpisná délka
16	SourcelpMetroCode	Další informace o zdrojové IP
17	SourcelpAreaCode	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

Hodnota pole *Ip\_address* odpovídá hodnotě v poli *Sourcelp*. Stejně tak si odpovídají pole *Threat*.

## Varianty malware b106

Označení	Popis
B106-Bladabindi	Bladabindi může odcizit citlivé informace a poskytnout je útočníkovi, může do podezřelého stroje stáhnout další malware
B106-CB	Podezřelý stroj je zasažen hrozbami Bladabindi a Jenxcus
B106-Jenxcus	Jenxcus může odcizit citlivé informace a poskytnout je útočníkovi, poskytuje útočníkovi přístup k podezřelému stroji
B106-MULTI	Podezřelý stroj je zasažen více druhy malware
B106-Zacusca	Zacusca může odcizit citlivé informace, stáhnout více malware nebo poskytnout přístup k podezřelému stroji útočníkovi
B106-*	<p><b>Zbylé hrozby spadající do rodiny malware označené jako b106 jsou:</b></p> <p><i>Agent, AgentBypass, Ainslot, Amighelo, Ardamax, Arhost, Assassin, AutInject, Autoac, Autorun, Balidor, Bancos, Bandok, Banker, Banload, Bariori, Beastdoor, Beaugrit, Bexelets, Bezigate, Bifrose, Binder, Bisar, Blohi, BrowserPassview, Cakl, Cashback, Ceatrg, Cechip, Ceelinject, Chir, Chuchelo, Comame, Comisproc, Comitsproc, Comrerop, Comroki, Comsirig, Coolvidoor, Coremhead, Crime, Danglo, Darkdoser, Darkmoon, Decay, Defsel, Delf, DelfInject, Delfsnif, Dimegup, Dokstormac, Dooxud, Dorkbot, Dusvext, Dynamer, Effbee, EyeStye, Fareit, Farfli, Folyris, Frosparf, Fynloski, Gamarue, Gaobot, Geratid, Gernidru, Geycript, Gratem, GSpot, Habbo, Hamweq, Hanictik, Hiderun, HistBoader, Horsamaz, Hoygunver, Hupigon, Inject, Injector, IRCbot, Ircbrute, Itsproc, Keygen, Keylogger, Kilim, Kkmaka, Klovbot, Knowlog, Ldpinch, Lenc, Leodon, Levitiang, Lybsus, Lypsacop, Mafod, Malagent, Malex, Meredrop, Mielit, Misbot, Mobibez, Mosripe, Mosucker, Msposer, Napolar, Naprat, Nayrabot, Necast, Neeris, Nemim, Neop, Neshta, Netbot, NetWiredRC, Neurevt, Nitol, Noancooe, Nosrawec, Nuqel, Nusump, Obfuscator, Otran, Parama, Parite, PcClient, Pdfjsc, Poison, Poisonivy, Pontoeb, Popiidor, PossibleMalware, Prorat, Prosti, Protos, Pushbot, Ramnit, Ranos, Rbot, Rebhip, Remhead, Rimod, Ritros, Runner, Sality, Scar, Sdbot, Sharke, Silby, SillyShareCopy, Sisproc, Sisron, Skypams, Small, Smpdoss, Sormoeck, Splori, Spybot, Squida, SSonce, Sulunch, Swisyn, Swrort, SynFlood, Tapazom, Tawsebot, Tearspear, Tendrit, Tenpeq, Tobfy, Tocojob, Toobtox, Tumpadex, Turkojan, Twores, Vahodon, Vake, VB, Vbencrypt, Vbinder, VBInject, Vburses, Vharke, Vinject, Virut, Vobfus, Vonriamt, Vtub, Weenkay, Wervik, Xtrat, Xyligan, Yemrok, Zbot, Zegost</i></p> <p><b>Jedná se o červy nebo trojské koně. Často obsahují komponenty s funkcí keyloggeru nebo mohou být použity k DDoS útoku.</b></p>