

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

### CITADEL

#### Stručná charakteristika

Některé varianty umožňují aktualizaci verze botnetu, aby se vyhnuly detekci antivirovou ochranou, protokolem XMMP. Provozovateli botnetu umožňuje například nahrávat video o činnosti uživatele, zaznamenávat stisknuté klávesy (keylogger), zjistit nainstalovaný software, využívat příkazovou řádku a tak dále. Botnet byl využit na různé operace od DDoS útoků, přes krádeže osobních dat až po krádeže z bankovních účtů.

Citadel je vylepšenou variantou botnetu Zeus. Sdílí s ním téměř 600 funkcí. Ke komunikaci s C&C servery využívá šifry RC4 a AES. Jednou z klíčových vlastností je blokování aktualizací antivirového software a také Windows Update.

Detailnější informace k tomuto botnetu naleznete v online dostupném dokumentu: [Malware analysis: Citadel](#).

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, 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 Citadel

Označení	Popis
B54-BASE	http spojení k doméně spojené s botnetem Citadel
B54-CONFIG	Spojení k doméně hostující konfigurační soubor malware Citadel
B54-INIT	
B54-OLD	Podezřelý stroj komunikoval se staršími doménami spojenými s malware Citadel
B54-CODE1	Podezřelý stroj pravděpodobně obsahuje aktivní malware Citadel
B54-DNS	IP adresa DNS serveru který používal stroj potenciálně nakažený malwarem Bamital. Nemusí se nutně jednat o nákazu.