ČD-TELEMATIKA

Internetové služby

ČDT-MONITOR

Služba ČDT-MONITOR umožňuje získat zákazníkovi přehled o bezpečnostních incidentech pocházejících od koncových uživatelů v jeho internetové síti. Prostřednictvím speciálních sond je monitorován internetový provoz odcházející od koncových uživatelů zákazníka a sebraná data jsou vyhodnocována metodami detekujícími bezpečnostní rizika. S tímto produktem získává zákazník rychlý přehled o bezpečnostních rizicích ve své síti (útoky generované z jeho sítě, skenování počítačů, generování spamu atd.), což mu umožňuje rychle reagovat a předcházet tak zneužívání zdrojů v jeho síti k DDoS útokům a rozesílání SPAMu, ale např. i zařazení jeho IP adres do veřejných blacklistů a ztrátě reputace.

www.cdt.cz

ČD - Telematika a.s. **Korespondenční adresa** Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz, poptavka@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-TELEMATIKA

Internetové služby

ČDT-MONITOR

Použité metody

- **Telnet** – zvýšené použití služby Telnet. Detekuje veškeré spojení, včetně pokusů o spojení na TCP port 23, a pro jednotlivé IP adresy počítá počty těchto spojení;
- **SSHDICT** – pokusy o uhodnutí uživatelského jména/hesla, případně přihlášení podvrženým certifikátem ke službě SSH. Metoda je schopna rozpoznat úspěšný/neúspěšný útok;
- **OUTSPAM** – odesílání nebo pokusy o odesílání zvýšeného počtu e-mailů z konkrétních IP adres;
- **SCANS** – různé typy scanování sítě a způsoby provedení. Součástí detailů je počet unikátních scanů, zpráva o případné odpovědi scanované IP adresy a seznam dotčených portů. Indikuje zavirované IP adresy v síti;
- **DNSQUERY** – zvýšený počet DNS dotazů z konkrétních IP adres;
- **DNSANOMALY** – podezřelá komunikace DNS provozu;
- **BLACKLIST** – kontrola provozu (podle přiřazených filtrů) a rozpoznání komunikace s IP adresami uvedenými na blacklistu;
- **RDP Dictionary Attacks** – rozpoznává pokusy o uhádnutí uživatelského jména a hesla do služby RDP. Slovníkové útoky jsou široce rozšířenou a oblíbenou metodou pro získání neautorizovaného přístupu do počítačového systému.
- **REFLECTDOS Amplificated DoS attack** – detekuje DoS útoky, které využívají ke svému zesílení nedostatků některých služeb. Umožňují vygenerovat pro specifický požadavek několikanásobně větší odpověď, a to k jejímu odeslání na podvrženou zdrojovou IP adresu požadavku (např. prostřednictvím nezabezpečených NTP serverů).

Hlavní výhody

- včasné odhalení rizikového provozu v internetové konektivitě
- snížení zátěže na aktivních prvcích provozovatele sítě
- další rozvoj obchodních aktivit velkoobchodních partnerů směrem ke koncovým zákazníkům

Komu je služba určena

- lokální poskytovatelé internetu
- velké a střední společnosti
- státní správa a samospráva

Služba je poskytována jako doplňková služba k přístupu do sítě internet, poskytované společností ČD - Telematika.

Ukázka reportu

ID	TIMESTAMP	P	EVENT TYPE	SOURCE	DETAIL	TARGET
#418...2504	2021-11-18 07:40:00	I	SCANS	[redacted]	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 1445, targets: 1419, port(s): 670, 671).	213.235.154.115 , 213.235.149.165 , 213.235.188.113 , 213.235.155.208 , ... more
#418...2500	2021-11-18 07:40:00	I	SMTPANOMALY	[redacted]	Mail count: 1205, network average: 328.02.	80.95.99.76 , 52.1.6.42 , 92.62.234.42 , 185.139.69.34 , ... more
#418...3246	2021-11-18 07:40:00	C	REFLECTDOS	[redacted]	Misuse of the device to the amplification DoS attack (service: domain, data sent: 54.31 MiB, data received: 123.36 KiB, outgoing connections: 42810).	45.236.150.152 , 51.195.44.116 , 68.111.135.29 , 69.110.44.199 , ... more
#418...2505	2021-11-18 07:40:00	I	SCANS	[redacted]	horizontal TCP SYN scan (attempts with response: 16, attempts without response: 1016, targets: 1032, port(s): 23).	85.13.118.56 , 85.13.117.167 , 85.13.94.179 , 85.13.117.40 , ... more
#418...1699	2021-11-18 07:37:25	I	DNSANOMALY	[redacted]	High amount of TCP DNS traffic, whole transfer: 55.79 KiB.	192.52.178.30
#418...1700	2021-11-18 07:35:16	I	DNSANOMALY	[redacted]	High amount of TCP DNS traffic, whole transfer: 21.66 KiB.	8.8.8.8
#418...1732	2021-11-18 07:35:00	I	SMTPANOMALY	[redacted]	SMTP [TCP/25] (unique hosts: 1, mail count: 1, legitimate server response).	2001:718:1001:149::155

www.cdt.cz

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz, poptavka@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938