Analýza síťového provozu

Ve společnosti XXXXXXXXXX

Vzorová zpráva

Tento dokument je interním dokumentem Linux Services, bez souhlasu autora nesmí být zveřejněn.

(Implementační scénáře a metodiky aktualizovány dle zákona o kybernetické bezpečnosti – NÚKIB a BSI - IT Grundschutz, Německo)

Ing. Michal Vymazal
Ing. Jiří Richter

Duben 2019

Obsah

Analýza síťového provozu

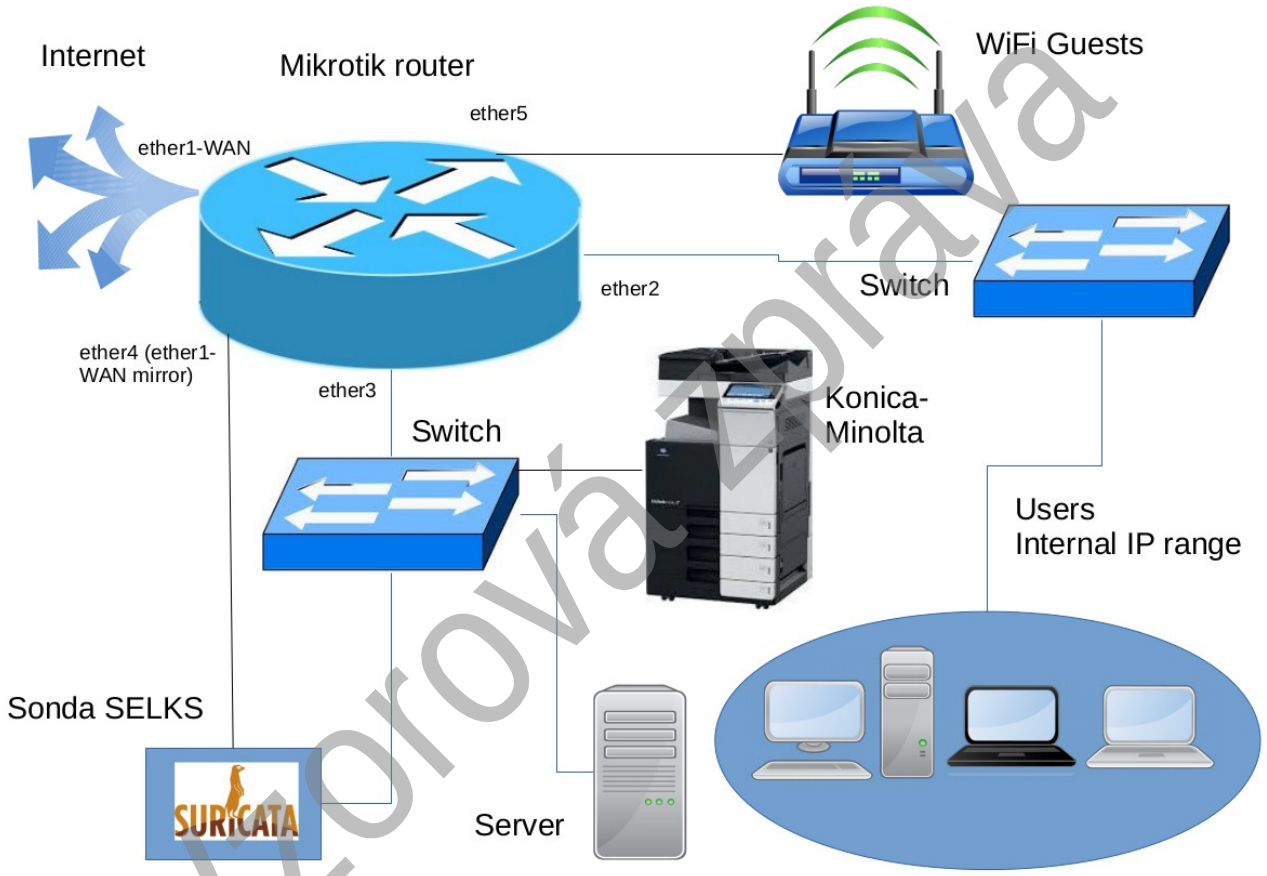
Analýza síťového provozu slouží pro vyhodnocení síťového provozu v dané lokalitě. Sondu je možné připojit do jakékoliv LAN nebo WAN sítě. Na základě výstupu ze sondy je možné provést vyhodnocení veškerého síťového provozu v dané lokalitě a určit, zda některé zařízení není např. napadeno škodlivým kódem, optimalizovat provoz jednotlivých zařizení, vyhodnotit stávající bezpečnostní opatření apod.

Veškerá analýza síťového provozu probíhá tzv. "pasivním odposlechem", kdy síťová sonda (Analyzátor síťového provozu na bázi programového vybavení Suricata) je připojena k Mirror portu zařízení (Switch, Router) na kterém měříme síťový provoz. Veškerý provoz je pak zaznamenán, analyzován a vyhodnocen. Nedochází k ovlivňování provozu, prolamování šifer atp.

Externí měřící bod, WAN

Sonda je připojena k WAN rozhraní externího routeru. Je zachycen veškerý síťový provoz směřující z routeru a interní LAN směrem do internetu a veškerý síťový provoz směřující směrem z internetu na WAN rozhraní routeru a dále veškerý síťový provoz směřující z internetu do vnitřní LAN sítě.

Topologické schema zapojení sondy



Sdílení síťových disků

Na externím měřícím bodu nebyly zachyceny žádné pakety obsahující data z protokolů SMB, NFS nebo jiných nešifrovaných protokolů určených pro síťové sdílení diskových kapacit. Tento nález hodnotíme **kladně**.

Identifikované nálezy

Nešifrovaný přístup k poště, poštovní klient

Vlastní komunikace mailového klienta s poštovním serverem není šifrovaná, je

možné sledovat celou komunikaci včetně uživatelského jména a přístupového hesla (user credentials)

Riziko

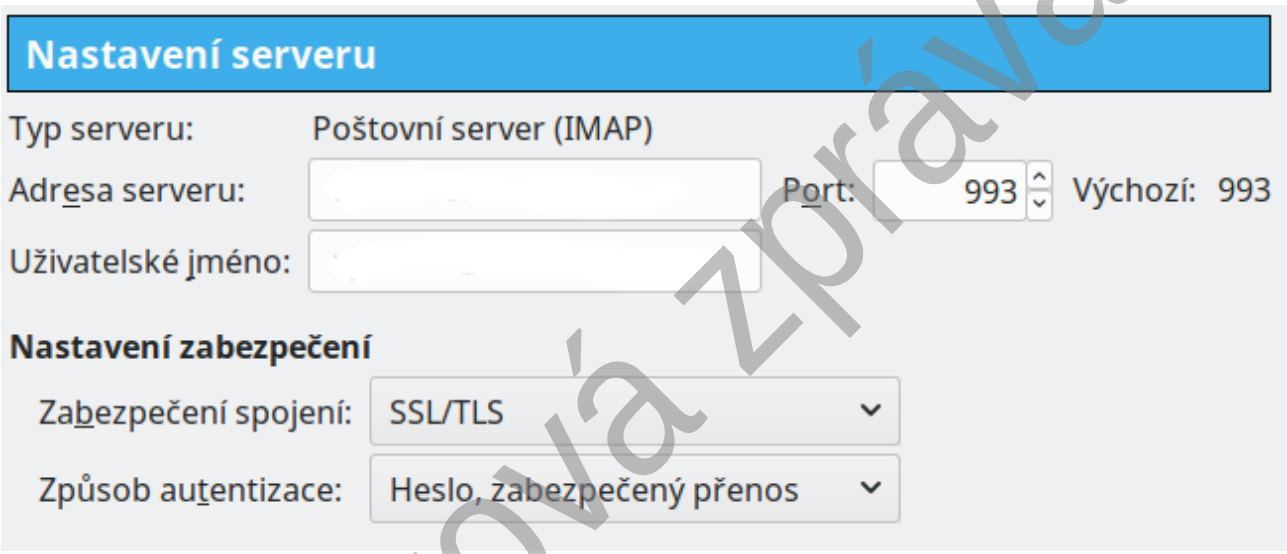
Vysoké

Možné dopady

Útočník může získat kopii mailové korespondence a tyto informace zneužít.

Doporučení

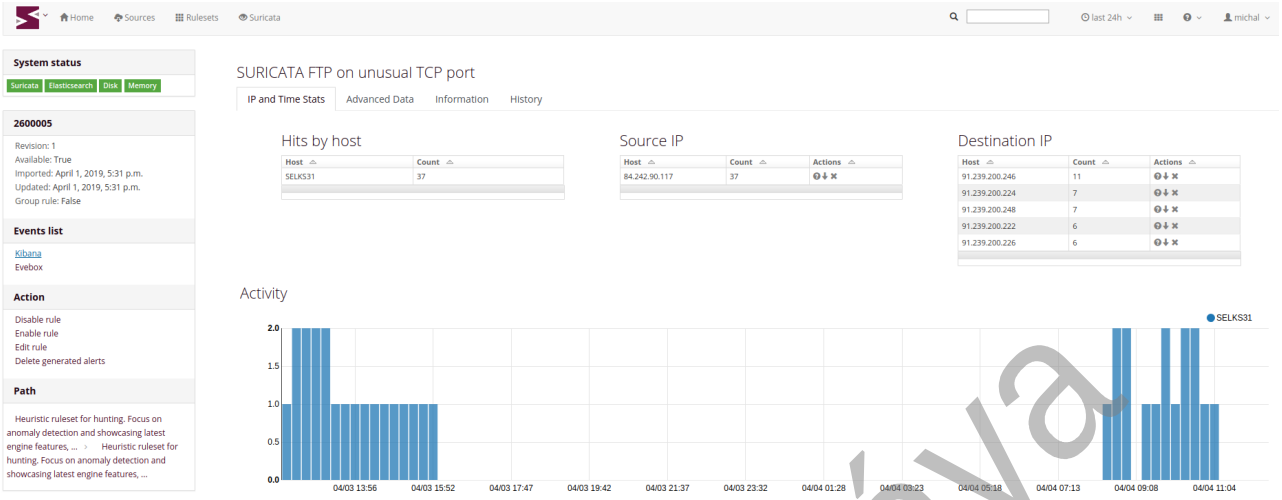
Přejít na šifrovanou komunikaci mailového klienta s poštovním serverem. Doporučujeme TLSv1.2



(Obrázek ve vzorové zprávě vynechán)

Ukázka analýzy spojení mailového klienta s poštovním serverem. Spojení není šifrované. Lze identifikovat uživatelský účet a heslo.

Četnost výskytu spojení mailového klienta s poštovním serverem. Spojení není šifrované.



Odesílání hesel v nešifrovaném tvaru, protokol HTTP

Komunikace se serverem není šifrovaná. Analýzou spojení lze získat uživatelské jméno a heslo k účtu.

Riziko

Vysoké

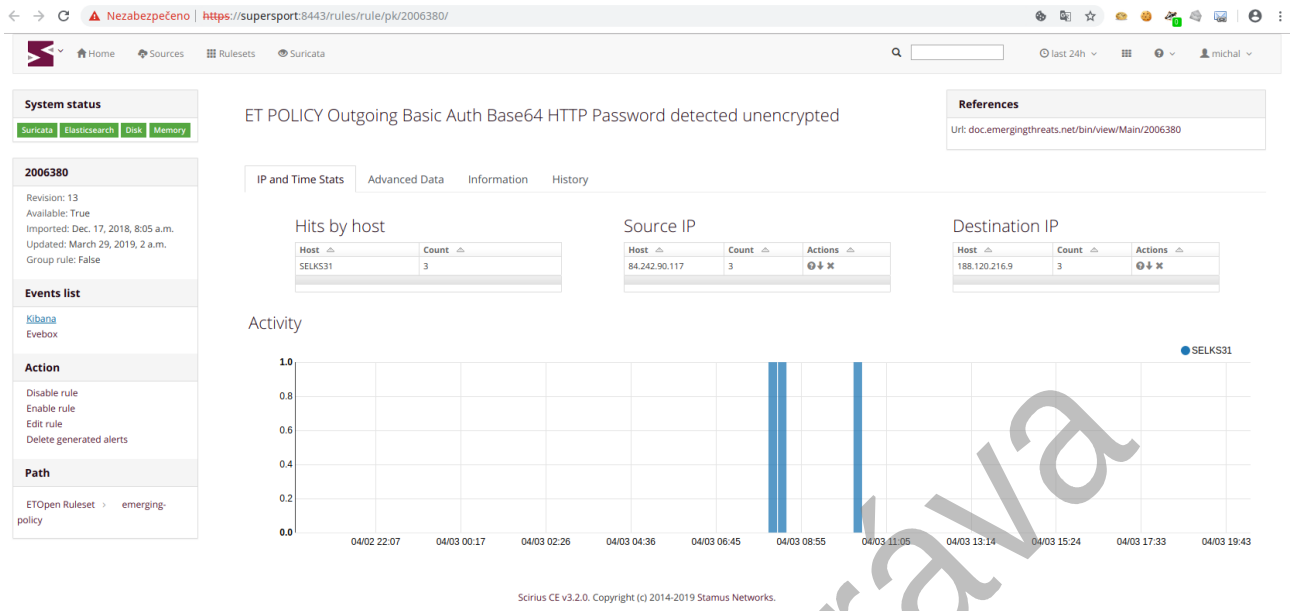
Možné dopady

Útočník může získat přihlašovací údaje k serveru a tyto informace zneužít.

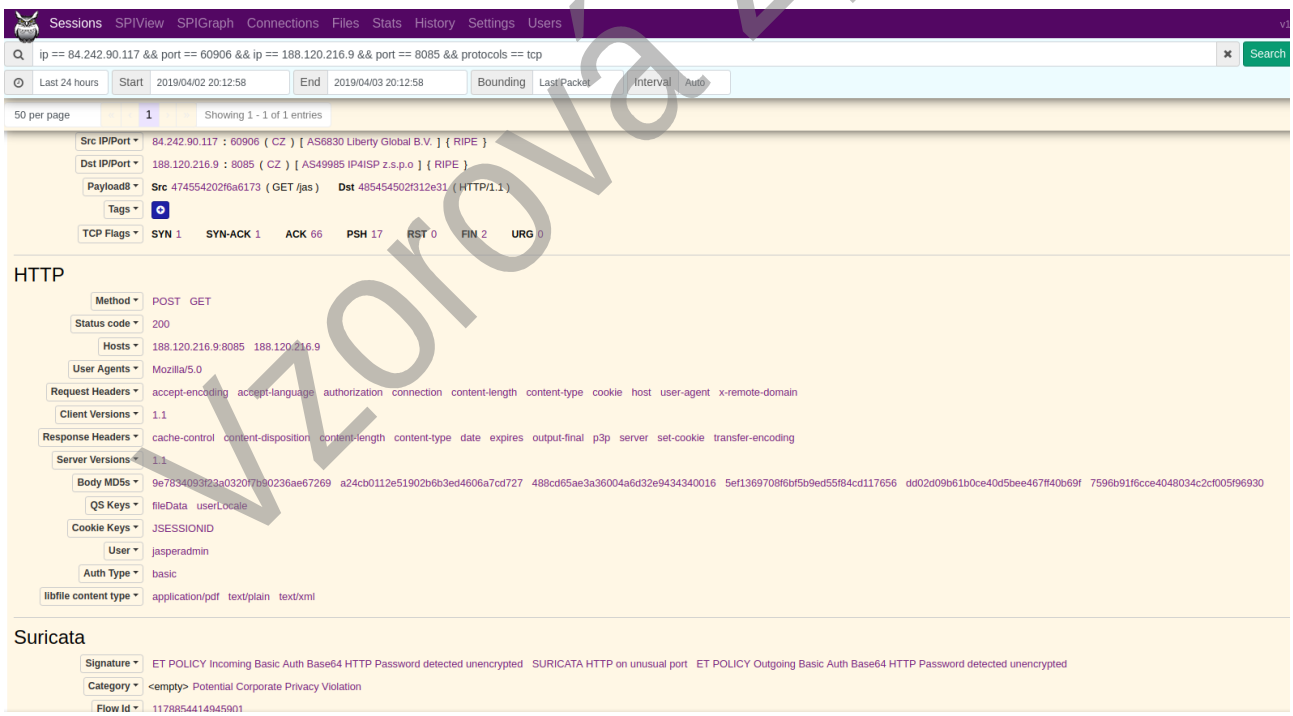
Doporučení

Nalézt zařízení, ze kterého spojení probíhá (viz. následující měření z interního měřícího bodu) a identifikovat aplikaci, která spojení provádí. Určit význam komunikace s tímto serverem.

Četnost výskytu nešifrovaného spojení na server xx.xx.xx.xx



Analýza spojení se serverem xx.xx.xx.xx. Je patrné uživatelské jméno.



Pokus o odeslání dat na servery Cloudflare

Dochází k neúspěšnému pokusu o odeslání dat na servery Cloudflare

Riziko

Střední

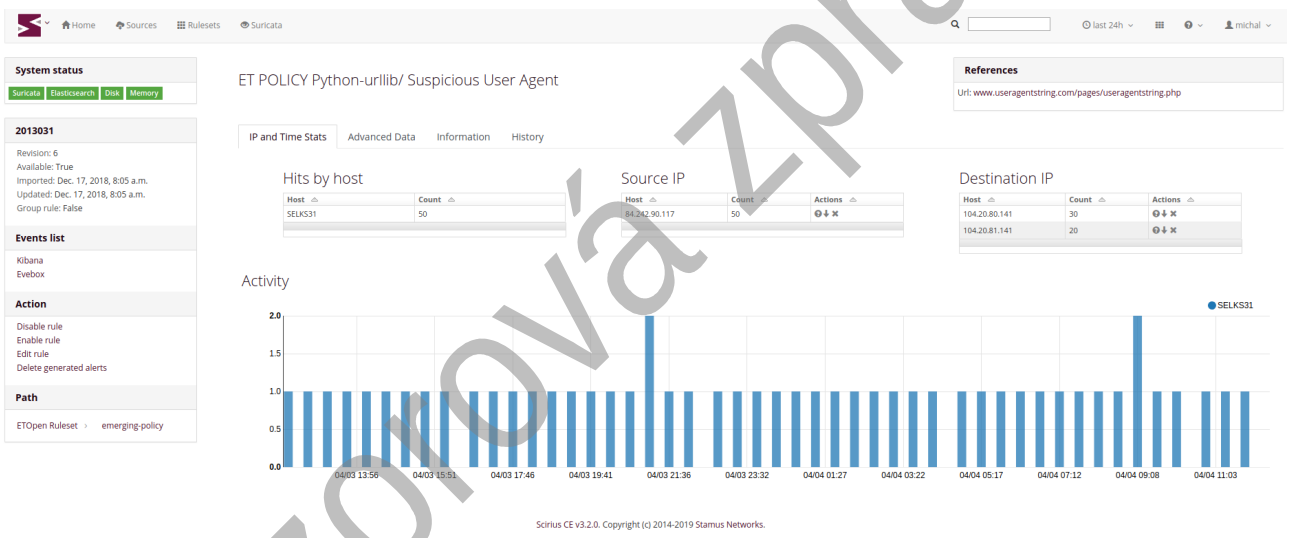
Možné dopady

Útočník může zíkat data z interní sítě.

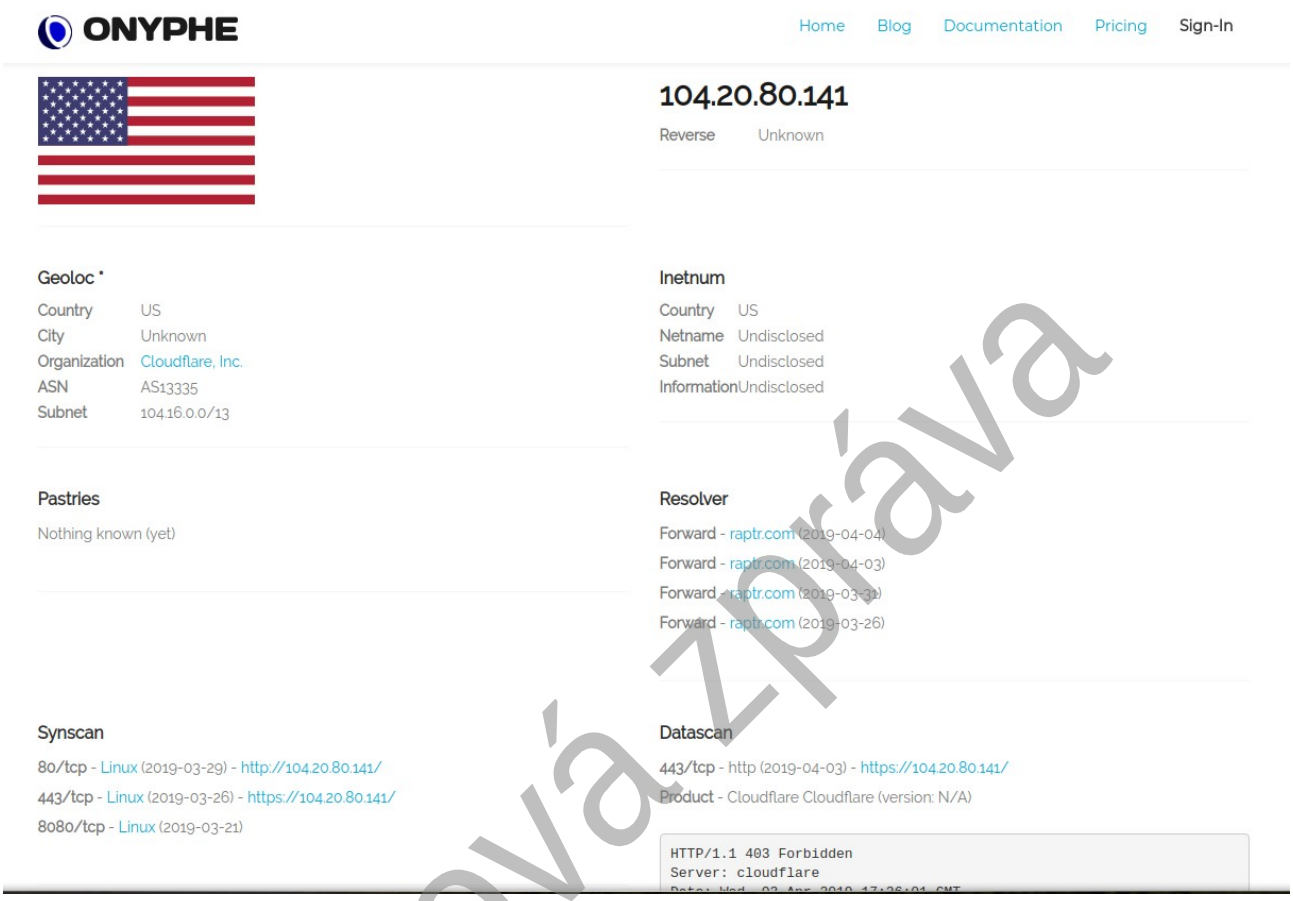
Doporučení

Nalézt zařízení, ze kterého spojení probíhá (viz. následující měření z interního měřícího bodu) a identifikovat aplikaci, která spojení provádí. Určit význam komunikace s tímto serverem.

Četnost výskytu komunikace se servery Cloudflare



Identifikace serveru Cloudflare



Poštovní klient, imap na portu 143

Poštovní klient "obsluhuje" poštu na poštovním serveru pomocí zastaralých šifrovacích mechanismů. Samotné šifrování na protokolu imap nemusí být příliš "odolné".

Riziko

Střední

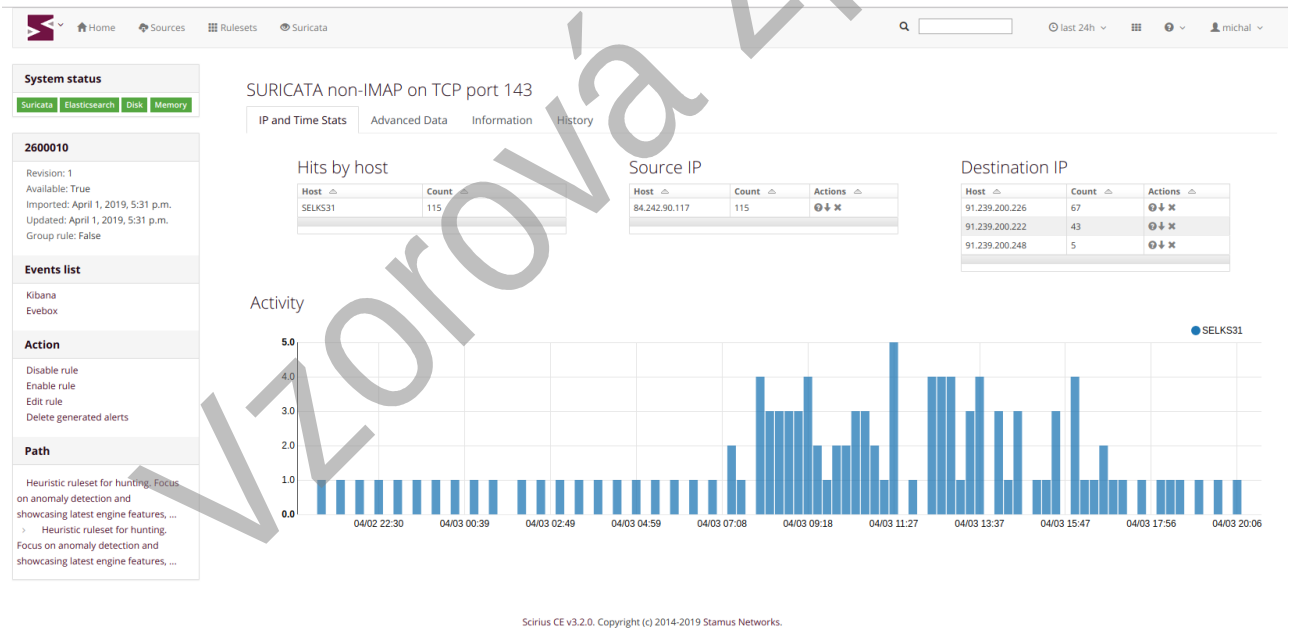
Možné dopady

Útočník může získat kopii mailové korespondence a tyto informace zneužít.

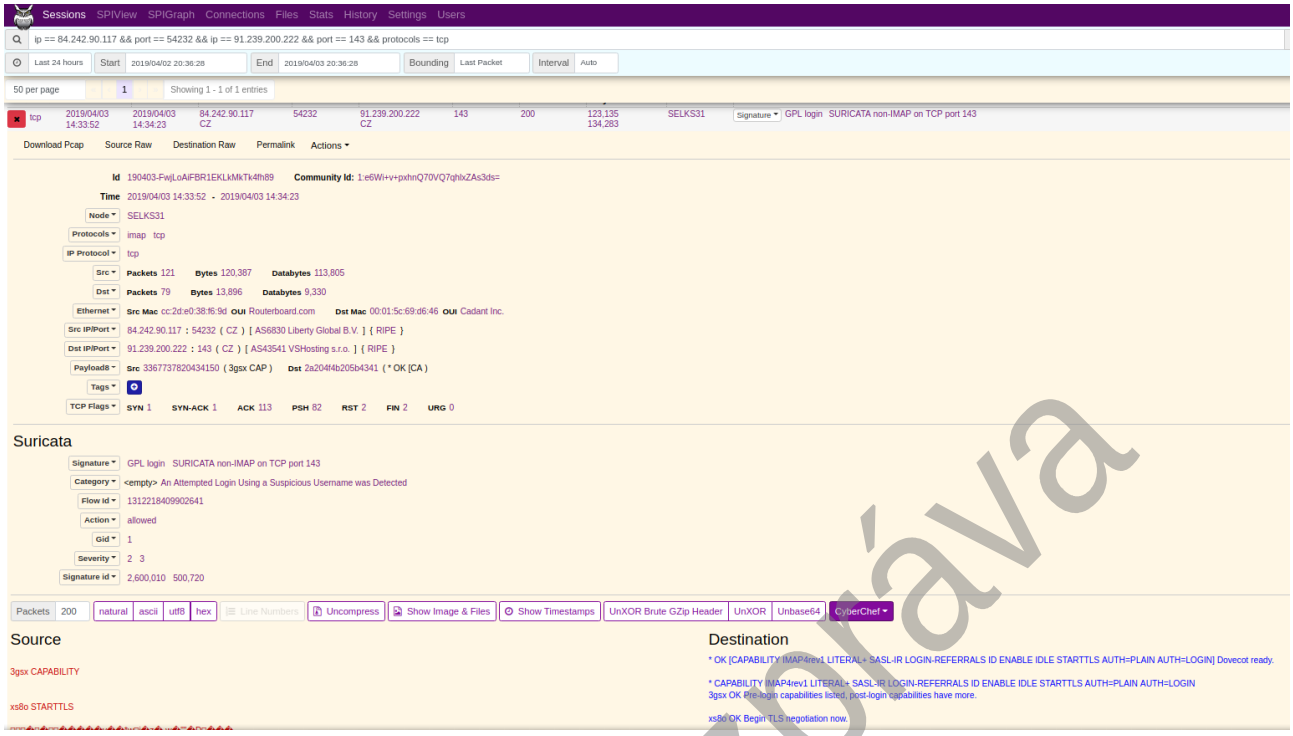
Doporučení

Přejít na šifrovanou komunikaci mailového klienta s poštovním serverem. Doporučujeme TLSv1.2. Viz. doporučení z kapitoly "Nešifrovaný přístup k poště, poštovní klient".

Četnost výskytu spojení

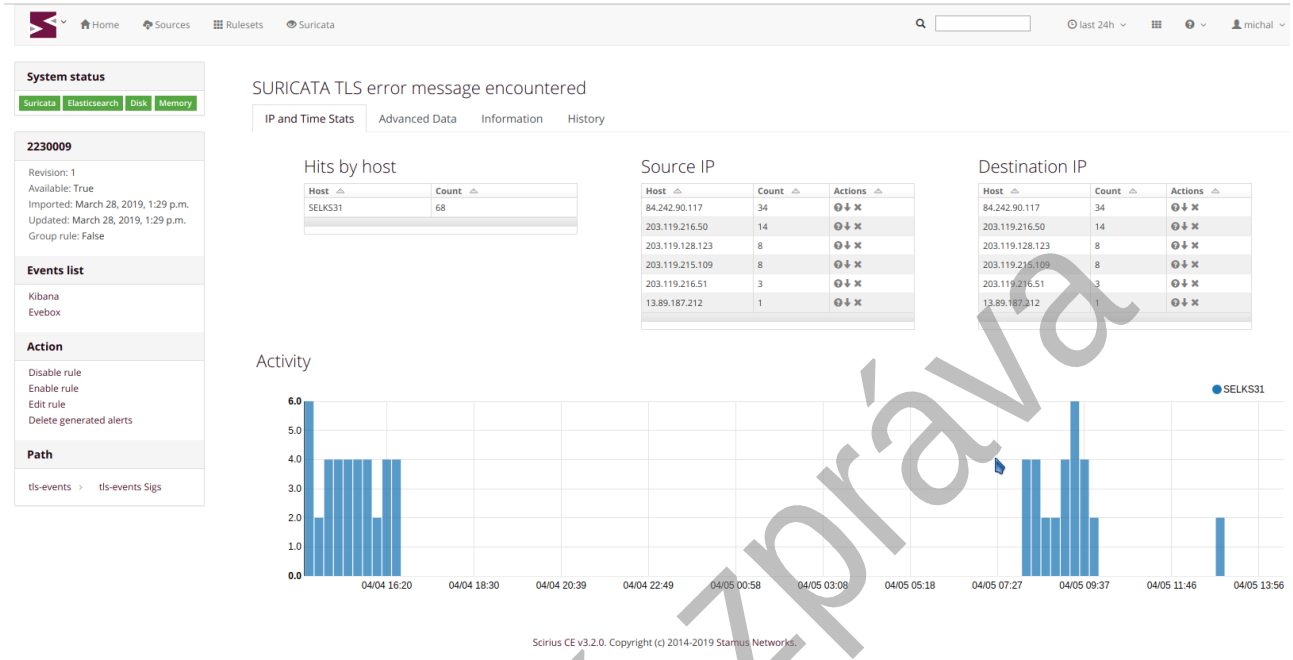


Analýza spojení poštovního klienta se serverem

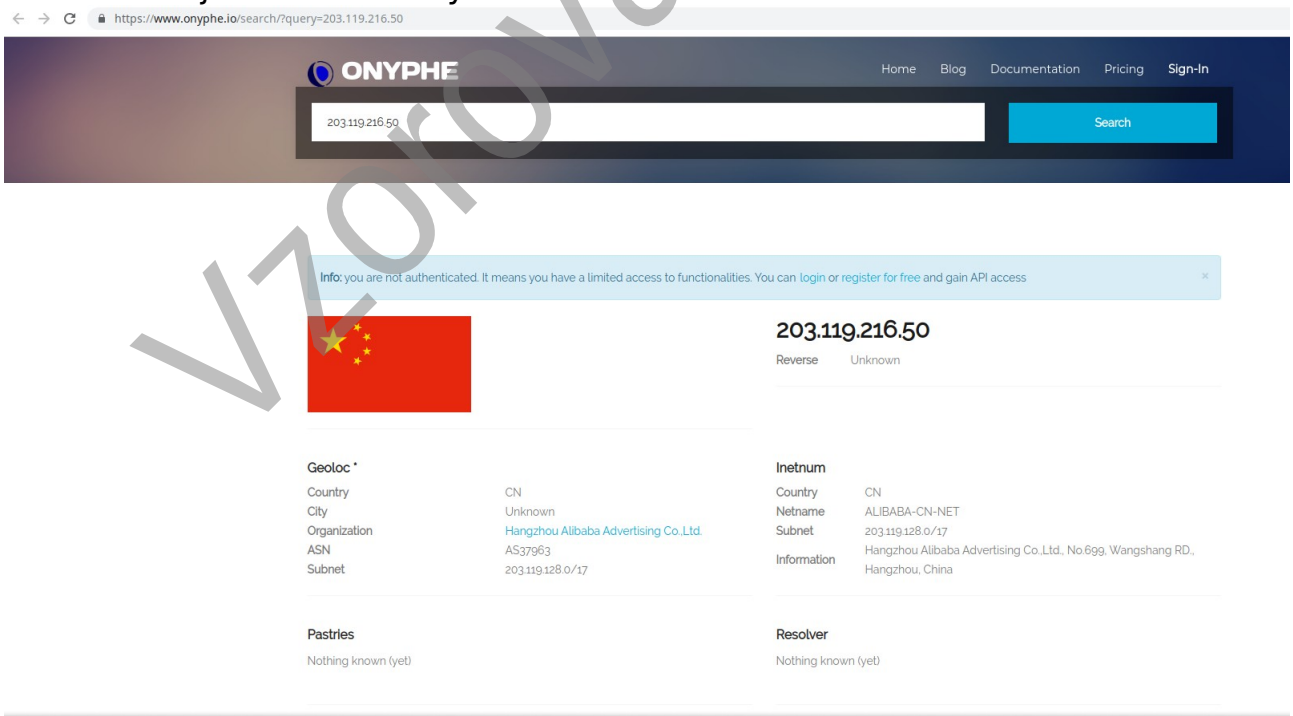


Neidentifikovaný provoz, zřejmě externí WiFi router

Byl nalezen neidentifikovaný datový provoz. Zařízení se pokoušelo odesílat data na čínské servery



Identifikace jednoho z čínských serverů



Ukázka datového toku na čínský server

2019-04-03 10:13:53 6 days ago	ALERT	S: 203.119.216.50 D: 84.242.90.117	SURICATA TLS error message encountered
2019-04-03 10:06:56 6 days ago	ALERT	S: 203.119.216.50 D: 84.242.90.117	SURICATA TLS error message encountered
2019-04-03 08:05:18 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 0; Bytes: 60; Packets: 1
2019-04-03 08:05:18 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 0; Bytes: 60; Packets: 1
2019-04-03 08:03:47 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 18; Bytes: 658; Packets: 7
2019-04-03 08:03:47 6 days ago	FLOW	S: 203.119.216.50 D: 84.242.90.117	TCP 203.119.216.50:443 -> 84.242.90.117:38014; Age: 18; Bytes: 658; Packets: 7
2019-04-03 08:01:09 6 days ago	ALERT	S: 203.119.216.50 D: 84.242.90.117	SURICATA TLS error message encountered
2019-04-02 16:24:04	ALERT	S: 203.119.216.50	SURICATA TLS error message encountered

Vylučovací metodou jsme dospěli k zařízení TP-LINK WIFI router. Po dohodě s provozovatelem routeru byl tento router odpojen. Při tomto kroku vyšel najevo fakt, že do „podezřelého“ routeru byla připojena zabezpečovací ústředna Jablotron. Vlastní zabezpečovací ústředna byla přepojena do přepínače (switch) ve vnitřní síti.

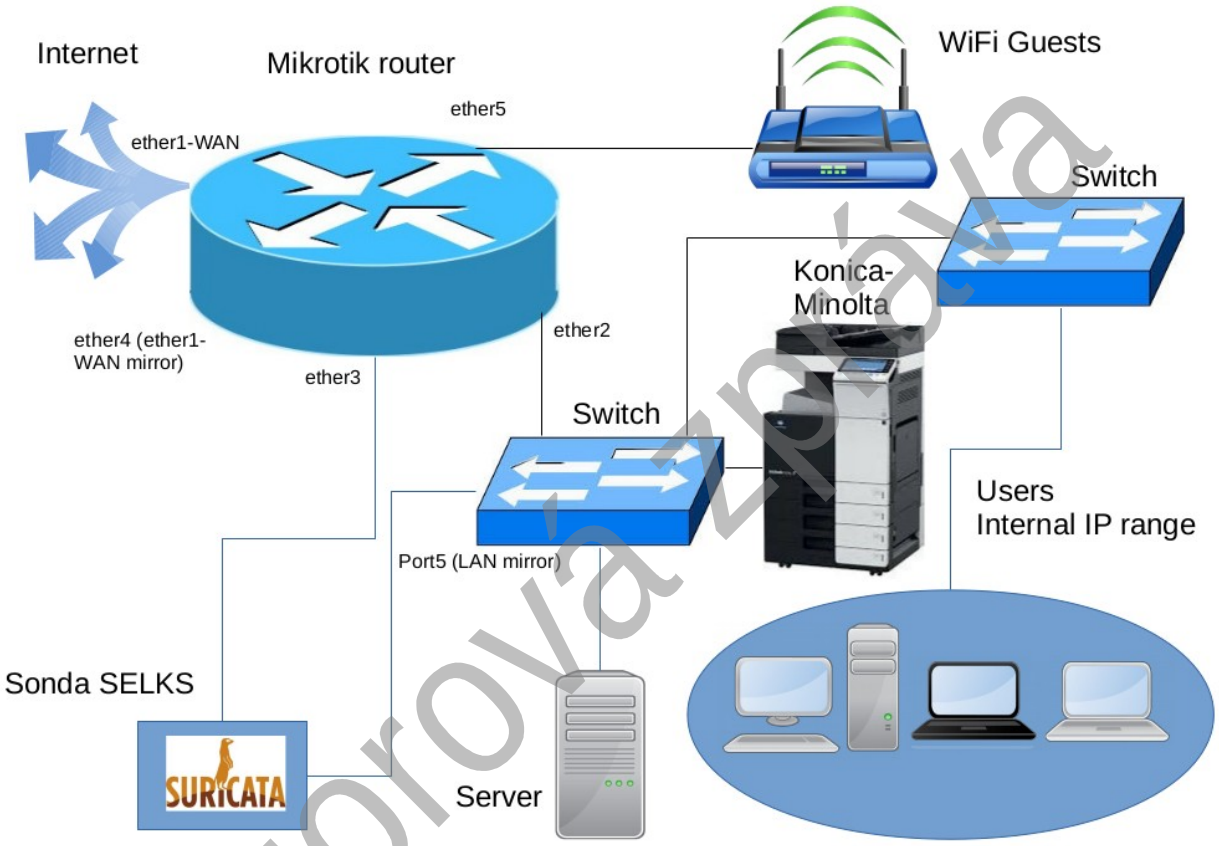
Poznámka

Toto zjištění hodnotíme jako velmi závažné, zabezpečovací ústředny (resp. jejich datový kanál) by nikdy neměly být připojeny k zařízením podobného typu. Do budoucna doporučujeme konzultovat připojení datového kanálu ústředny s výrobcem zabezpečovací ústředny.

Interní měřící bod, vnitřní LAN

Sonda je připojena k LAN rozhraní interního přepínače. Je zachycen veškerý síťový provoz v interní LAN a dále veškerý síťový provoz směřující z interní LAN do internetu a veškerý síťový provoz směřující z internetu do interní LAN.

Topologické schema zapojení sondy



Identifikované nálezy

Odesílání hesel v nešifrovaném tvaru, protokol HTTP

Komunikace se serverem není šifrovaná. Analýzou spojení lze získat uživatelské jméno a heslo k účtu.

Riziko

Vysoké

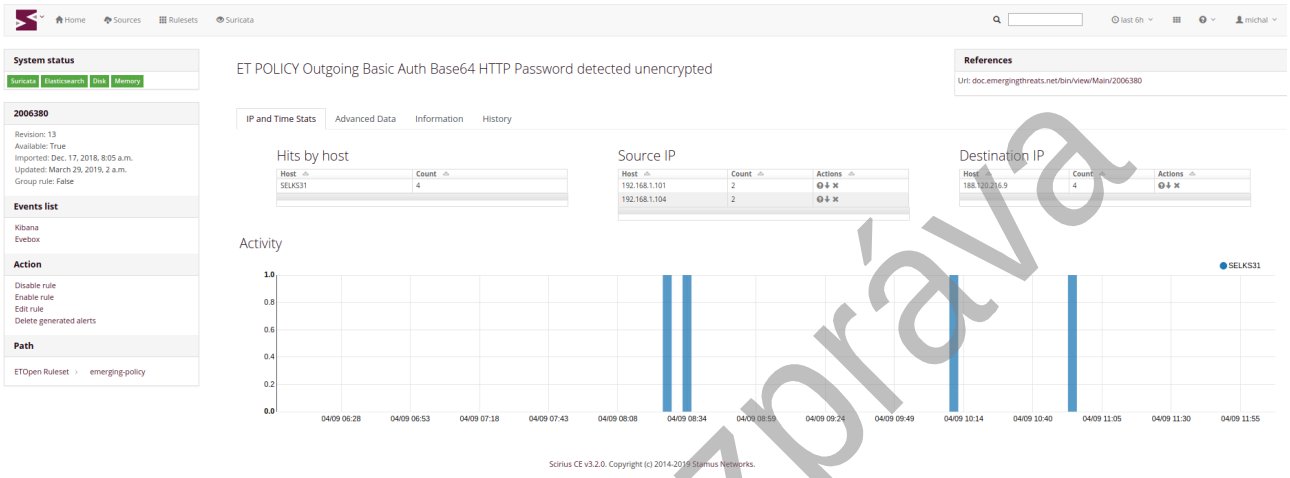
Možné dopady

Útočník může zíkat přihlašovací údaje k serveru a tyto informace zneužít.

Doporučení

Jedná se o stroje 192.168.1.101 a 192.168.1.104. Na straně serveru je pravděpodobně hotelový rezervační systém. Spojení není šifrováno, na straně serveru je možné identifikovat položky jako "Pokladna".

Spojení se serverem xx.xx.xx.xx



Pokus o odeslání dat na servery Cloudflare

Dochází k neúspěšnému pokusu o odeslání dat na servery Cloudflare

Riziko

Střední

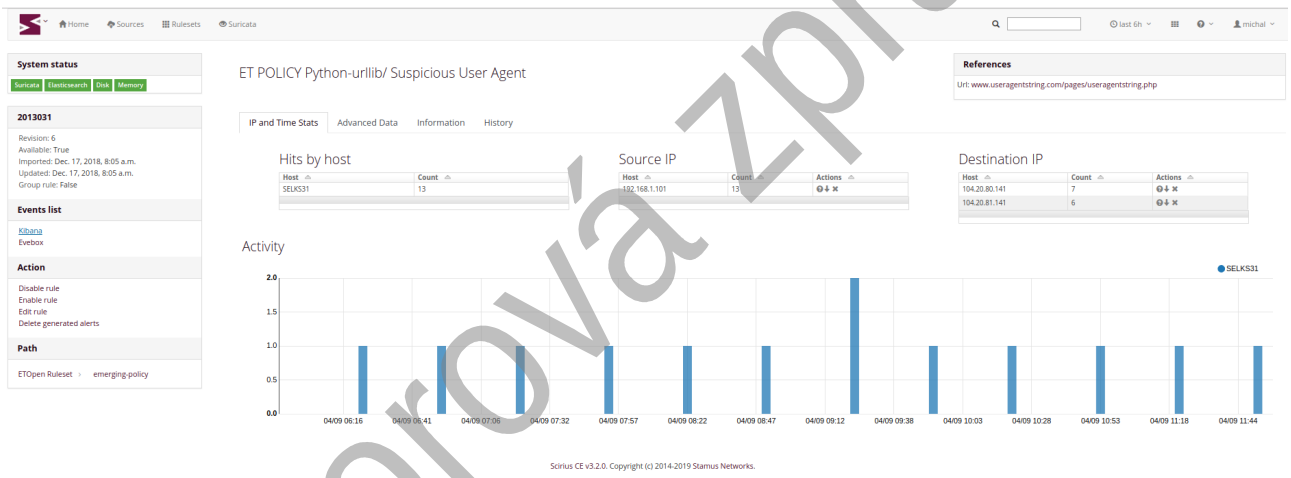
Možné dopady

Útočník může zíkat data z interní sítě.

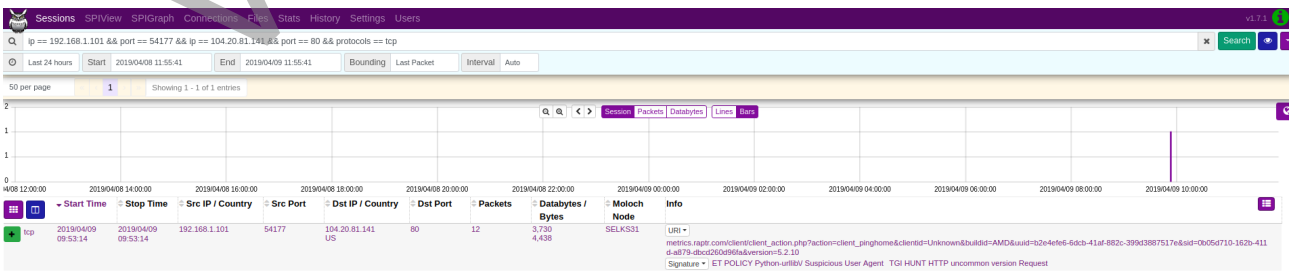
Doporučení

Jedná se o zařízení s IPv4 interní adresou 192.168.1.101. Je třeba určit význam komunikace s tímto serverem.

Četnost výskytu komunikace se servery Cloudflare



Analýza spojení se serverem Cloudflare



Tiskárna, odesílající data na internetový server

Tiskárna Konica Minolta (IPv4 192.168.1.13) odesílá data na server 195.234.183.240, tato IPv4 adresa je registrována na Konica Minolta Business Solutions Europe GmbH. Data jsou šifrována v rámci protokolu TLSv1.0. Nelze vyloučit, že v rámci odesílaných dat jsou zahrnuty i dokumenty na této tiskárně vytištěné nebo skenované.

Riziko

Střední

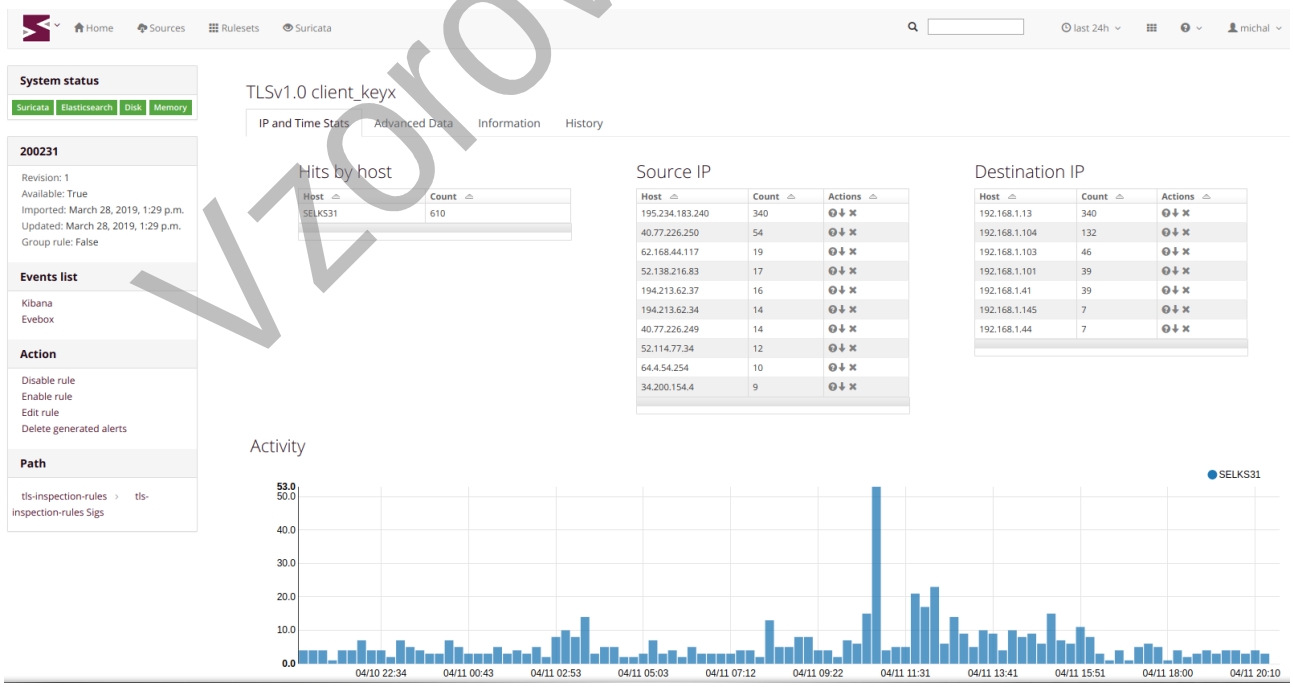
Možné dopady

Útočník může získat data z interní sítě.

Doporučení

Doporučujeme zvážit využití multifunkčního zařízení (tiskárna, scanner), které bude autonomní a nebude vysílat data z interní sítě na servery v internetu.

Tiskárna Konica Minolta (IPv4 192.168.1.13) odesílá data na server 195.234.183.240, zbylé public IPv4 adresy patří společnosti Microsoft nebo Google.



Počítače, odesílající data na internetový server

Některé uživatelské stanice odesílají data na internetové servery společnosti Microsoft nebo Google (obrázek viz. Předchozí obrázek). Data jsou šifrována v rámci protokolu TLSv1.0. Nelze vyloučit, že v rámci odesílaných dat jsou zahrnuta i data nad rámec běžné telemetrie.

Riziko

Střední

Možné dopady

Útočník může získat data z interní sítě.

Doporučení

Doporučujeme vypnout na všech stanicích odesílání telemetrických dat na servery technologických společností (Google, Microsoft aj.)

Doporučení jednotlivých opatření

Sdílené datové úložiště (sdílení souborů)

Doporučujeme sdílet datové soubory prostřednictvím privátního datového úložiště. Vhodná je například technologie Nextcloud (https://nextcloud.com/about, https://www.linuxservices.cz/owncloud). Vlastní přenos dat mezi klentem a serverem je vždy šifrován, data mezi klientem a serverem jsou synchronizována automaticky).

Stávající Samba server doporučujeme vyřadit a již dále nepoužívat. Samba server používá pro komunikaci s jednolivými stanicemi nešifrovaný protokol, rovněž je problematické ověřování a vystavování přístupových práv k jednotlivým souborům na serveru. **Dále doporučujeme vyřadit služby pro sdílení pevných disků na pracovních stanicích.**

Data ze samba serveru lze zmigrovat na nextcloud server. Tento převod je bezeztrátový.

Pevné vnitřní IPv4 adresy pro jednotlivé (nepřenosné) uživatelské stanice

V současnosti uživatelské stanice dostávají přiděleny vnitřní IPv4 adresy od DHCP serveru. Tato praxe způsobuje, že stejnou IPv4 adresu může postupně získat více uživatelských stanic. V případě jakékoliv anomálie je pak obtížné identifikovat stanici dle IPv4 adresy. Doporučujeme každé uživatelské stanici (jedná se o nepřenosné stroje) přidějit pevnou IPv4 vnitřní adresu a tyto adresy zanést do provozního deníku spolu s popisem (názvy) jednotlivých stanic. Přenosná zařízení budou nadále dostávat IPv4 vnitřní adresy prostřednictvím DHCP serveru.

Hardening www prohlížečů na uživatelských stanicích

Doporučujeme provést hardening www prohlížečů na uživatelských stanicích. Viz. https://www.linuxservices.cz/hardening

Zákaz IPv6 provozu na všech zařízeních

Některá zařízení mají povolen IPv6 provoz. Doporučujeme vypnout podporu pro IPv6 na všech zařízeních. Na řadě zařízení není v současné době podpora IPv6

dobře implementována a povolení IPv6 tak může představovat bezpečnostní hrozbu.

Vypnutí ladících funkcí na všech zařízeních

Některá zařízení (patrně přenosné telefony a tablety) mají evidentně povoleny ladící funkce. V případě šifrovacích knihoven toto znamená i povolení TLS režimu

Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Pokud bude mít tento režim zároveň povolený i server, pak může v rámci vyjednávání parametrů pro šifrované spojení na bázi TLS dojít k tomu, že přenos dat mezi zařízením a serverem nebude šifrován.

Vystavení bezpečných (doporučených) parametrů pro šifrované tunely (IKE, IPSEC)

Analýzou šifrovaného spojení na bázi IKEv1, IPSEC bylo zjištěno, že některé kanály mají jako alternativu povoleny i parametry 1024 modp group (Diffie Hellmann) a 3DES symetrický šifrovací algoritmus. Oba tyto parametry již dnes nejsou považovány za bezpečné a jsou zakázány. Doporučujeme každému IKE, IPSEC kanálu vystavit samostatný předpis s doporučenými parametry (IPSEC tunnel mode) dle těchto dokumentů

IKEv1

NÚKIB - Doporučení v oblasti kryptografických prostředků

https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickych-prostredku/

IKEv2

BSI TR-02102-3 "Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)" Version: 2019-1

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-3.pdf

Slovníček pojmů

Zkratka	Vysvětlení zkratky
Audit IS	Vlastním auditem informačního systému rozumíme proces jehož výstupem je zdokumentování informačního systému, popis jeho vazeb na okolní informační systémy a prostředí.
	Metodika BSI pro audit informačního systému https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile
Analýza rizik	Metodika sloužící k rozpoznání, předpovězení a vyhodnocení jednotlivých hrozeb a jejich dopadů na daný informační systém. Analýza rizik navazuje na vlastní bezpečnostní proces a představuje zpětnou vazbu pro daný informační systém a oblasti tímto informačním systémem dotčené.
	Výstupní dokument je třeba periodicky aktualizovat https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html
BIA	Business Impact Analysis
	Analýza dopadů (BIA) je základem celého procesu řízení kontinuity činností organizace (Business Continuity Plan, BCP). http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.html
BSI	*Bundesamt für Sicherheit in der Informationstechnik*
	Německá národní bezpečnostní autorita (obdoba českého NÚKIB). www.bsi.bund.de
DRP	Disaster Recovery Plan
	Jedná se o metodiky a postupy sloužící k obnově funkčnosti informačního systému po živelných pohromách a jiných zásadních událostech.
ISO	International Organization for Standardization
	Označení mezinárodní normy http://www.iso.org/iso/home.html
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
	www.nukib.cz
NIST	National Institute of Standards and Technology, USA
	http://www.nist.gov/
Penetrační testy	Cílem penetračních testů je odhalení zranitelností cílového informačního systému, stanovení způsobu jejich možného využití a doporučení vedoucí k jejich nápravě.
	http://www.linuxservices.cz/penetracni-testy