TRAFICOM

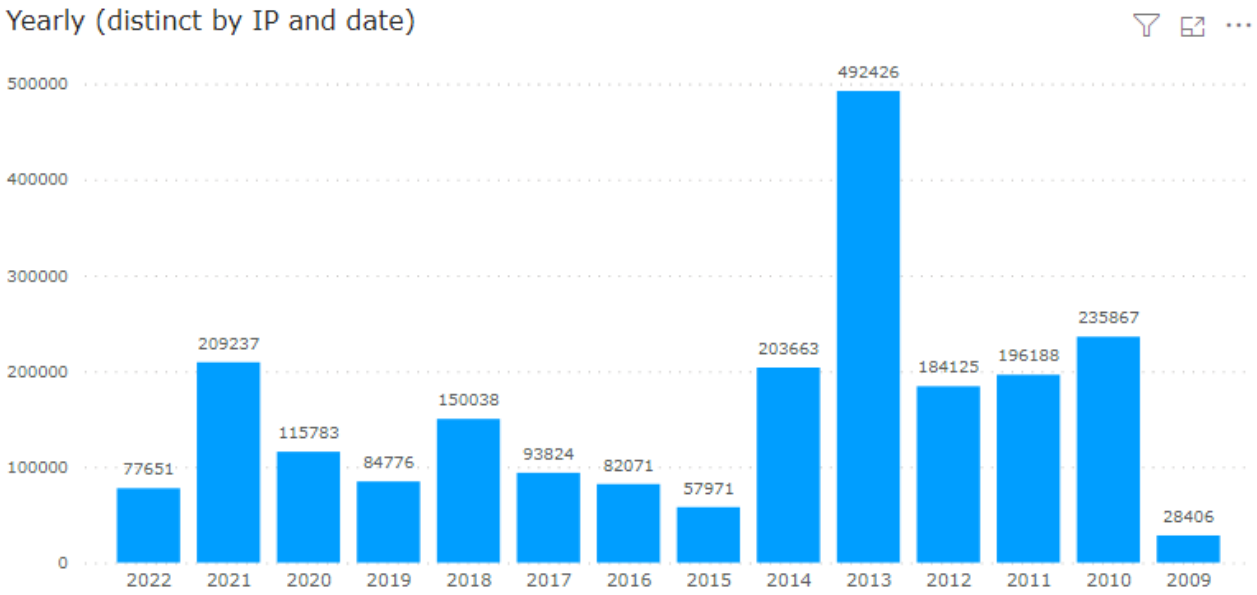
Finnish Transport and Communications Agency
National Cyber Security Centre

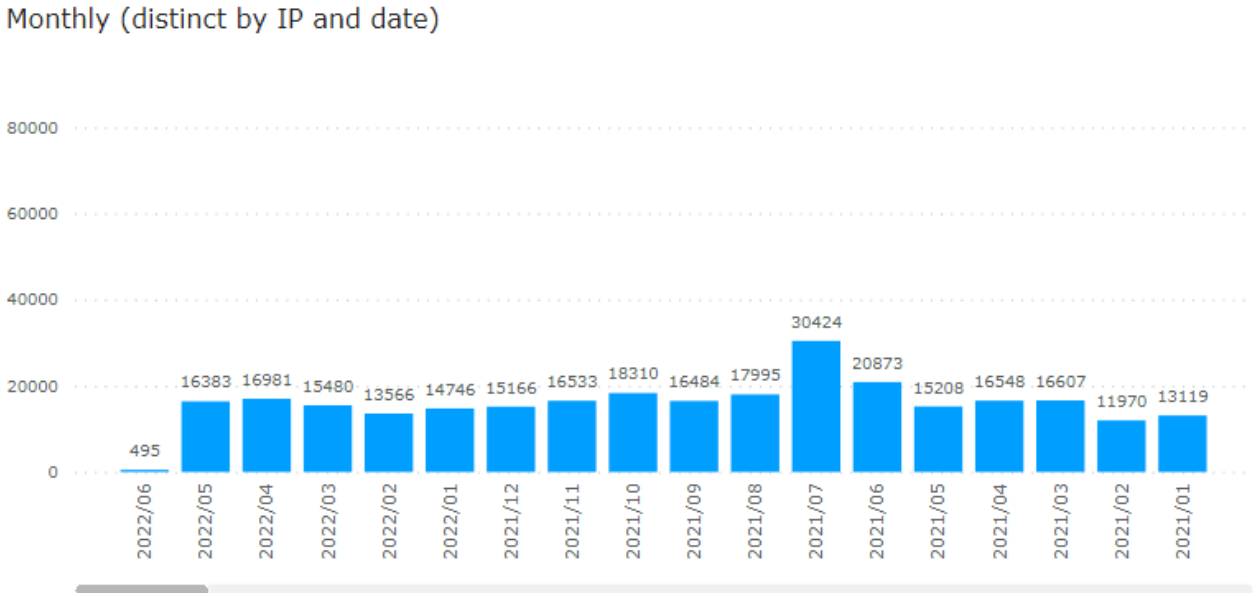
Handling open/vulnerable services in Finnish networks

Jussi Eronen

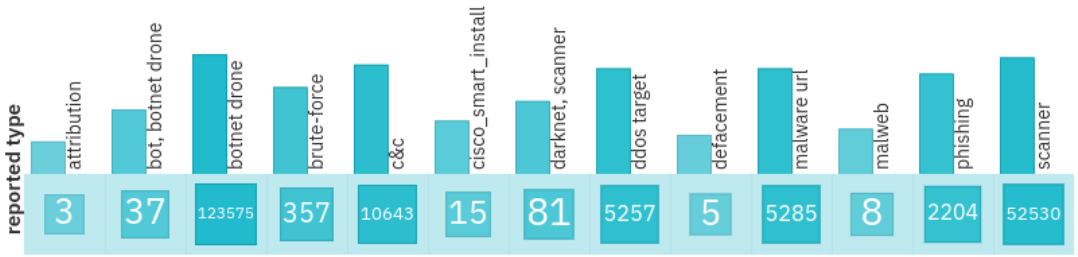
Autoreporter

- The project has been a great at handling botnets, phishing, and other malicious content.
- But what about the rest of the data we gather: open and vulnerable services?

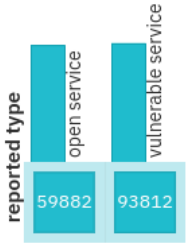




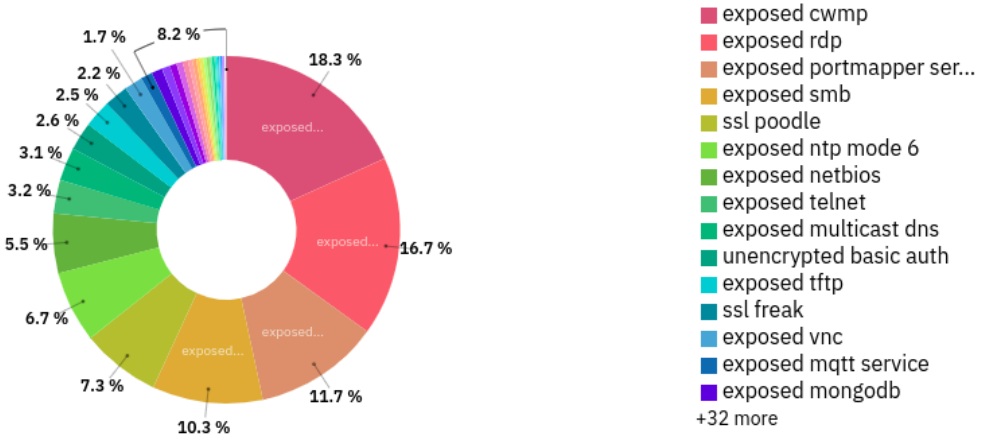
storage/events: filtered by ("reported type" != "open service" and "reported type" != "vulnerable ... 4 of 8 hours



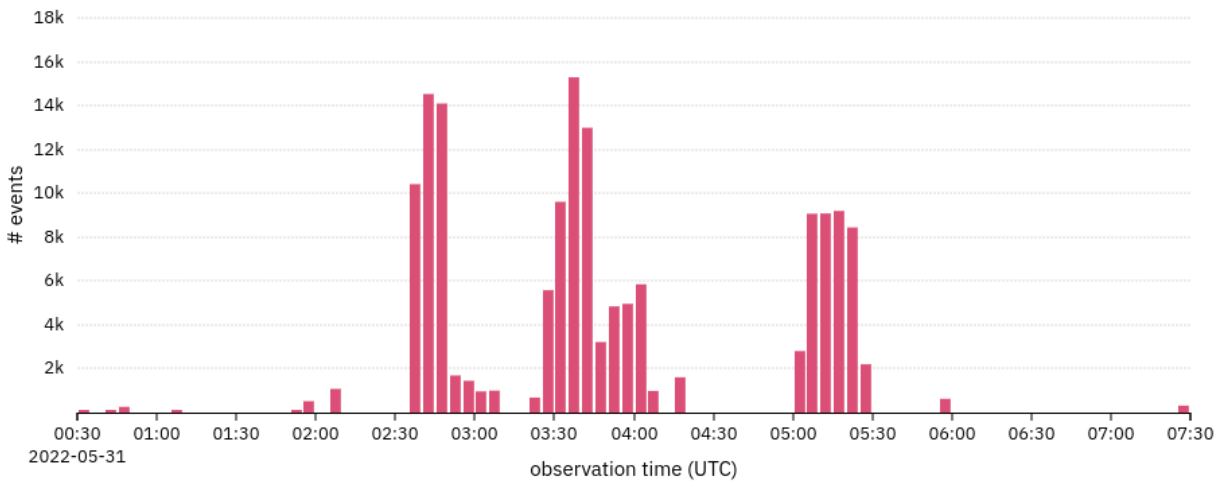
storage/events: filtered by ("reported type" == "open service" or "re... 2022-05-31 00:00:00 - 2022-05-31 23:59:59



vulnerable services: # events grouped by (vulnerability) 2022-05-31 00:00:00 - 2022-05-31 23:59:59



storage/events: filtered by ("reported type" == "open servi... 2022-05-31 00:00:00 - 2022-05-31 23:59:00



TRAFICOM

payload bytes of the request. [2] [3]

The following is a list of known protocols and their associated BAFs. CISA offers thanks to Christian Rossow for providing this information. For more information on BAFs, please see Christian's blog and associated research paper.

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—
WS-Discovery	10 to 500	—

In March 2015, the CERT Coordination Center of the Software Engineering Institute issued Vulnerability Note VU#550620 describing the use of mDNS in DRDoS attacks. Attackers can leverage mDNS by sending more information than can be handled by the device, thereby causing a DoS condition. [8]

In July 2015, Akamai Technologies' Prolexic Security Engineering and Research Team (PLXsert) issued a threat advisory describing a surge in DRDoS attacks using RIPv1. Malicious actors are leveraging the behavior of RIPv1 for DDoS reflection through specially crafted request queries. [9]

Total amplification (reports received 2022-05-31)

- Chargen: 130 * 358.8
- LDAP: 409 * (46+55)/2
- Memcached: 142 * (10000+51000)/2
- MDNS: 2889 * (2+10)/2
- NetBIOS: 5202 * 3.8
- NTP: 6290 * 556.9
- Portmapper: 10693 * (2+7)/2
- SSDP: 692 * 30.8
- QOTD: 24 * 140.3
- TFTP: 2408 * 60

- **TOTAL: 8 078 919 (28879 targets)**

(rough estimate, misses a lot of things such as middleboxes)

storage/events: filtered by ("reported type" == "open service" or "reported type" == "vulnerable service")

2022-05-31 00:00:00 - 2022-05-31 23:59:59

# events	product vendor	product
111341		
6579	ASUS	
3474	Fortinet	FortiGate
3062	Traefik Labs	Traefik
2508	F5	BIG-IP
2110	WatchGuard	Fireware
2019	NGINX	Kubernetes Ingress Controller
1422	Cisco	
1267	WatchGuard	Fireware XTM
1188		VNC protocol 3.8
1167	SonicWall	
1084		RabbitMQ
974	MikroTik	
926	CWP	CentOS Web Panel
654	Teltonika	
583	VMware	ESX Server
501	Philips	Hue
497	Fortinet	
494	Citrix	NetScaler
476	OPNsense	
470	Palo Alto Networks	GlobalProtect
365	Pulse Secure	Pulse Connect Secure VPN
359	Hikvision	
356	Check Point	
334	Cisco	IOS
329	Sophos	
321	VMware	ESXi Server
315	Dell	iDRAC
311	Cisco	ASA
296	Zyxel	ZyWALL USG 20
294	Synacor	Zimbra Collaboration Suite
289	QNAP	

TRAFICOM

“Finnish networks”?

$ cut -d ';' -f 1 ip-ranges-asns.txt | sort | uniq | wc -l

240

$ wc -l ip-ranges.txt

1204 ip-ranges.txt

$ cut -d '/' -f 2 ip-ranges.txt | awk '{sum+=2^(32-$1)}END {print sum}'

15 411 456

Autoreporter has ISP:s as the contacts

We could (and have) also tried to contact the customers directly

TRAFICOM

```
% Information related to '192.49.0.0 - 192.49.28.255'

% Abuse contact for '192.49.0.0 - 192.49.28.255' is 'abuse@tieto.com'

inetnum:        192.49.0.0 - 192.49.28.255
netname:        VTKK-ASIAKKAAT
descr:          Keilalahdentie 2-4
descr:          FI-02150 Espoo
descr:          Finland
country:        FI
```

Valtion tietokonekeskus

Valtion tietokonekeskus (lyhenne **Vtkk**, lempimi Vetski) oli valtiovarainministeriön alainen laitos, joka hoiti valtionhallinnon tietojenkäsittelytehtäviä. Vtkk perustettiin vuonna 1964. 1990-luvulla se ensin muutettiin liikelaitokseksi ja sen jälkeen yhtiöitettiin VTKK-yhtymä Oy:ksi. Vuoden 1996 alussa se fuusioitiin Tietotehdas Oy:n ja Unic Oy:n kanssa TT Tieto Oy:ksi (nyk. TietoEVRY Oyj).

Vtkk:n tehtävänä oli tarjota valtionhallinnon yksiköille niiden tarvitsemia tietotekniikkapalveluja omakustannushintaan. Näitä palveluja oli tietojärjestelmien määrittely, suunnittelu ja toteutus sekä konekeskuspalvelut. Pien- ja mikrotietokoneiden yleistyessä VTKK alkoi myös toimittaa laitteistoja asiakkailleen.

Vtkk:n suuria asiakkaita olivat muun muassa Autorekisterikeskus (ARK), sittemmin Ajoneuvohallintokeskus (AKE), nykyisin Liikenteen turvallisuusvirasto (Trafi), verohallinto, Väestörekisterikeskus (VRK), poliisi ja Valtiokonttori. VTKK ylläpiti valtionhallinnon suuria keskusrekistereitä kuten esimerkiksi Väestörekisteriä ja Ajoneuvorekisteriä. Valtionhallinnon yksiköillä oli VTKK:n toiminta-aikana velvollisuus käyttää VTKK:n palveluja, ellei muulle ratkaisulle ollut perusteltuja syitä, kuten omaa toteutusta, VTKK:n resurssivaikeuksia tai muuta sellaista.

How to do better?

Juhani.eronen@traficom.fi

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre