



DNS

91.3%

of malware uses
DNS in attacks



68%

of organizations
don't monitor
recursive DNS

Source: Cisco Security Research

DNS-Tunneling wird von verschiedenen APT-Gruppen eingesetzt

Die mit dem Iran verbundene APT-Gruppe OilRig nutzt DNS-Tunneling in hohem Maße für ihre Cyberspionage-Kampagnen

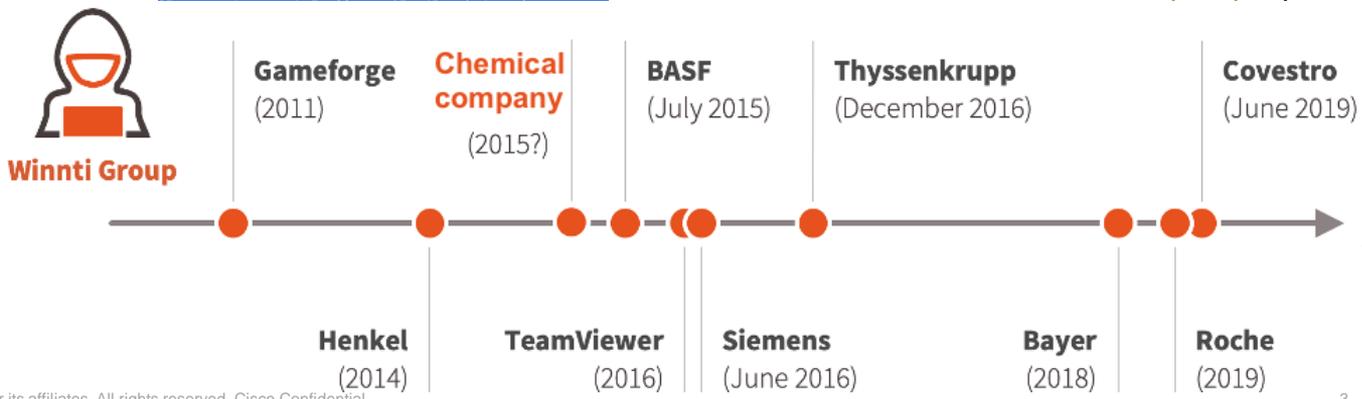
```

lnit.nbswy3dpfv3w64tmmxh16dupqzta.base32.tun2.test.com.
0.ccf3pgbiu6.ypp2e3hf4.1chncymr3e.sogrz.tun2.test.com.
1.sircpzxlw4.u6nyjr3pyh.4e55g5xlnk.iznsa.tun2.test.com.
unhg.kehgfb6ia6.xpjga.tun2.test.com.
o5k5.wlejfa64n.kyife.tun2.test.com.
gkjt.azn3bf27yv.gb2ub.tun2.test.com.
3pny.4lzspfn3z.6mtds.tun2.test.com.
tqv3.d5swkurwbb.zh5ay.tun2.test.com.
eg7mlk.ajag2.tun2.test.com.
4gmbu.dcg2v.tun2.test.com.
6tph2s.dea7k.tun2.test.com.
kr6ns.4gnkramjcy.52hpt.tun2.test.com.
11.tizaktcq5k.dscf4swwnv.74pragsk2w.x7mr2.tun2.test.com.
12.i9gerhx5fd.4okqc3hr7v.exp7vfszqk.lcedj.tun2.test.com.
13.z6bglfay7.gohjhzax3z.skwhmt7qab.j66zn.tun2.test.com.
14.d2j6hhv234.uinokao5km.rqjfgylkva.w2efx.tun2.test.com.
15.ymeoysh3sg.v2wo2ermpg.swcjvtjmeex.zayhr.tun2.test.com.
16.hgh3tco7tr.d6zacc25k4.rzhrchpxop.1bac
17.3amhsxgfoe.sh67axl.jmv.gycow4hpev.5gdx
18.cfeewg5ipn.bwl48vfvnr.bys1zh5ihl.zozr
19.wp6our7oww.yungf3moq6.j4peie4144.edww
20.jnhqnybuor.tz7lyw55o1.5vroppvfxm.f2fb
21.1enxkz25g.4gtcylawf7.6prz2ssvu.gfEb
22.4mm6wef6be.biopwvwtz.gssxdmn25y.z47ei
23.mbksn1zrve.7wjku7pbqb.55kjnv7avh.7dcb
24.4oyzsy4pg.oj5mwb3sbu.16m2fv3mjw.1dguo.comz.poo.com.
25.lzz7bby7bk.127lqp33qj.ye7v2slpcd.6r7gc.tun2.test.com.
26.h3kzc43qky.6dx7u3y31.rm747hbeyj.qibj6.tun2.test.com.
    
```



File Types
txt, jpg, png, pdf, mov...

WINNTI (auch bekannt als APT41, BARIUM und Blackfly) basiert auf einem DNS-Tunneling-Kommunikationskanal mit einer benutzerdefinierten Implementierung



Neue TLDs

- [.dad](#)
- [.phd](#)
- [.prof](#)
- [.esq](#)
- [.foo](#)
- [.zip](#)
- [.mov](#)
- [.nexus](#)



Gezielter Angriff

1. https://github.com/mysql/mysql-server/blob/8.0/mysql-test/std_data/data57.zip
2. https://github.com/mysql/mysql-server/blob/8.0/mysql-test/std_data/@data57.zip

1. https://github.com/mysql/mysql-server/blob/8.0/mysql-test/std_data/data57.zip
2. https://github.com/mysql/mysql-server/blob/8.0/mysql-test/std_data/@data57.zip

Beispiele

- microsoft-office[.]zip
- gmailbackup[.]zip
- paypal[.]zip
- payslip-statement[.]zip
- eicar-test-file[.]zip
- google-drive[.]zip

Power of Umbrella

microsoft-office.zip UNTERSUCHEN

microsoft-office.zip Malware -Sperrliste

Bedrohung Bedrohungstyp
- -

Inhaltskategorien Sicherheitskategorien
- Malware Phishing

[Einspruchskategorisierung](#)

Risikowert
 **100** Hohes Risiko
Die Domäne wurde aufgrund einer Kombination aus hohen Sicherheitsfunktionen als „Hohes Risiko“ eingestuft.

Erstellt am Land/Region der registrierten Person
13.05.2023 US

Letzte IP	Land/Region - IP	Präfix	ASN	Beschreibung des Netzwerkbesitzers
-	-	-	-	-

google-drive.zip UNTERSUCHEN

google-drive.zip Malware -Sperrliste Talos Google VirusTotal

Bedrohung Bedrohungstyp
- -

Inhaltskategorien Sicherheitskategorien
Not Actionable Malware

[Einspruchskategorisierung](#)

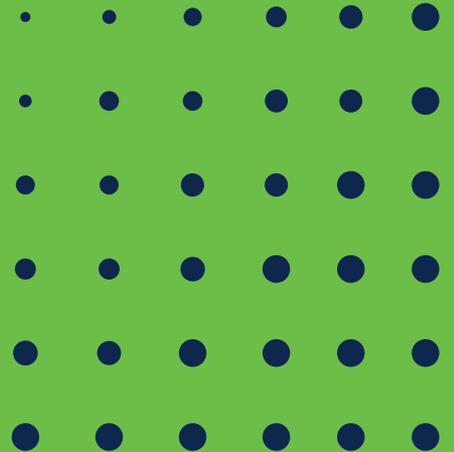
Risikowert
 **100** Hohes Risiko
Die Domäne wurde aufgrund einer Kombination aus hohen Sicherheitsfunktionen als „Hohes Risiko“ eingestuft. [▶ SICHERHEITSINDIKATOREN](#)

Erstellt am Land/Region der registrierten Person
16.05.2023 CA

Letzte IP	Land/Region - IP	Präfix	ASN
217.160.194.125	DE	217.160.0.0/16	AS8560

Beschreibung des Netzwerkbesitzers
IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE 86400 [ALLE IP ANZEIGEN \(1\)](#)

Newly Seen Domains



Newly Seen Domains

```
def generate_domain(year: int, month: int, day: int) -> str:
    """Generate a domain name for the given date."""
    domain = ""
    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFFF) << 17)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFFF8)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFFE) << 12)
        domain += chr(((year ^ month ^ day) % 25) + 97)
    return domain + ".com"
```

- For example, this method would generate the domain name **intgmxdeadnxuyla.com**, while the following day, it would return **axwscwsslmiagfah.com**. This simple example was in fact used by malware like [CryptoLocker](#).

Malicious queries in one month

14,584,007,454	Malware
2,752,747,377	Cryptomining
1,337,594,957	Phishing
1,156,240,139	Command and control
96,819,003	Newly seen domains

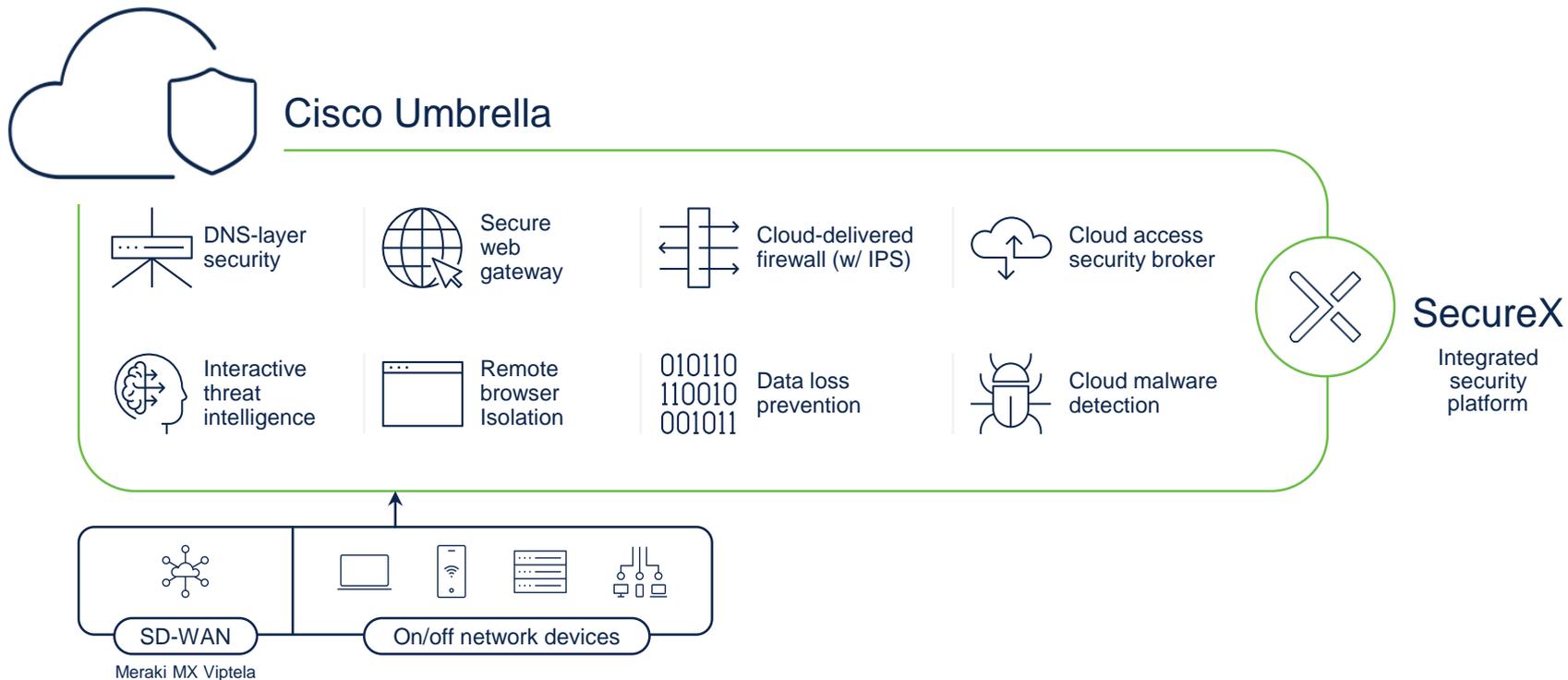
The screenshot shows the 'Security Settings' configuration page for a 'Default Policy'. Under the 'Categories To Block' section, there is a list of categories. The 'Newly Seen Domains' category is highlighted with a red arrow. The categories listed are:

- Malware: Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.
- Newly Seen Domains: Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks: Prevent compromised devices from communicating with attackers' infrastructure.
- Phishing Attacks: Fraudulent websites that aim to trick users into handing over personal or financial information.
- Dynamic DNS: Block sites that are hosting dynamic DNS content.
- Potentially Harmful Domains: Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN: VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
- Cryptomining: Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

At the bottom right, there are 'CANCEL' and 'SET & RETURN' buttons.

Cisco Umbrella

Visit our website to learn more



Demo

#fingercrossed





The bridge to possible