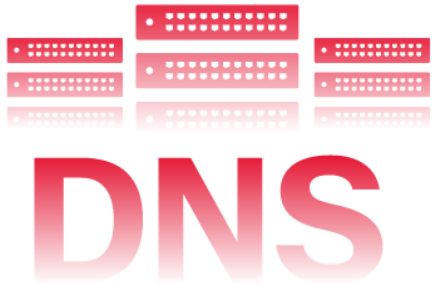
CISCO
SECURE

CISCO The bridge to possible

DNS-Security

Dirk Eberwein
Cybersecurity Sales Specialist



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

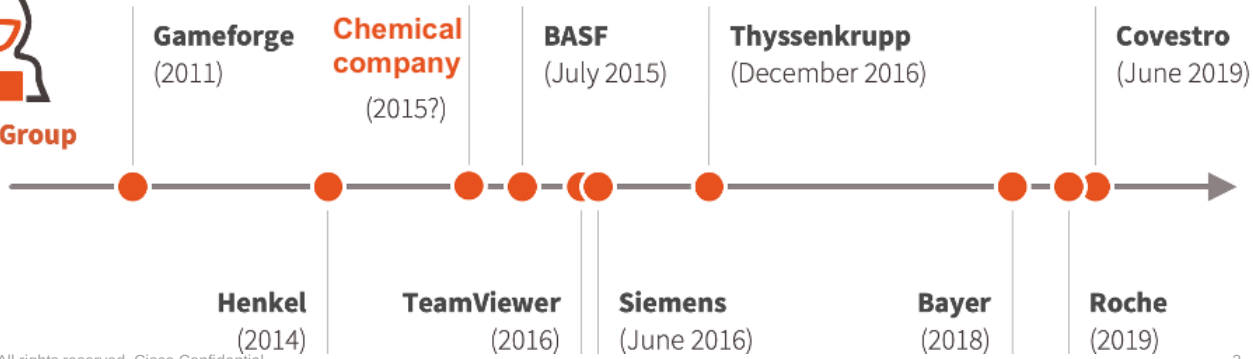
```
init.nbswy3dpfv3w64tmmqxhi6dupqzta.base32.tun2.test.com.
0.ccf3pqbiu6.ypfp2e3hf4.lchncynr5e.soqrz.tun2.test.com.
1.sircpzxlw4.u6nyjr3pyh.4e55g5xlnk.iznsa.tun2.test.com.
                unhg.kehqfb6ia6.xpjga.tun2.test.com.
                o5k5.wlejfba64n.kyife.tun2.test.com.
                gkjt.azn3bf27yv.qb2ub.tun2.test.com.
                3pny.4lzspfng3z.6mtds.tun2.test.com.
                tyv5.q5swdurwbb.zh5ay.tun2.test.com.
                pg7mlk.ajag2.tun2.test.com.
                z4qmbu.dcq2v.tun2.test.com.
                6tph2s.dea7k.tun2.test.com.
                kr6ns.4gnkramjcy.52bpt.tun2.test.com.
11.trzabtcq5k.dscf4swwnv.74pragsk2w.x7mr2.tun2.test.com.
12.i5qsrhx5fd.4okqc3hr7v.ewp7vfsrqk.lcedj.tun2.test.com.
13.z6bgflqay7.gohjhzsx3z.skwhmt7qab.j66zn.tun2.test.com.
14.d2j6hhv234.uinokao5km.rqjfqyikva.w2efx.tun2.test.com.
15.ymeoysb3sg.v2wo2ermpg.swcywtjmex.zayhr.tun2.test.com.
16.hqh3tco7tt.d6zacx25x4.rzbrchpxop.ibsc
17.3smhsrgfoc.sh67axljmv.gycow4hpev.5q4x
18.cfeewg5ipn.bwi45evfwr.bysizb5uhl.zorr
19.wp6our7oww.yungf3moq6.j4peie4144.edww
20.jnbqmybuor.tz7ywd55ol.5vccppvfxn.f2fb
21.lenxkxzs5g.4gtdylxwf7.6prm2eswnu.gefb
22.4nm6wmf6be.bio6wwwtzg.qssrdmnz5y.r47e
23.mbksniznvs.7wjku7pbqb.55kjnv7avh.7dxb
24.4oyrsyy4pg.oj5mvb3sbu.i6mzfw3mjw.ldgu
25.lrz7bby7tk.127iqp33qj.ye7v2slpcd.6r7qt.tun2.test.com.
26.h3kzc43qky.6dx7u3sy3i.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

Winnti Group



Picture from https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/

Neue TLDs

- .dad
- .phd
- .prof
- .esq
- .foo
- .zip
- .mov
- .nexus

Gezielter Angriff

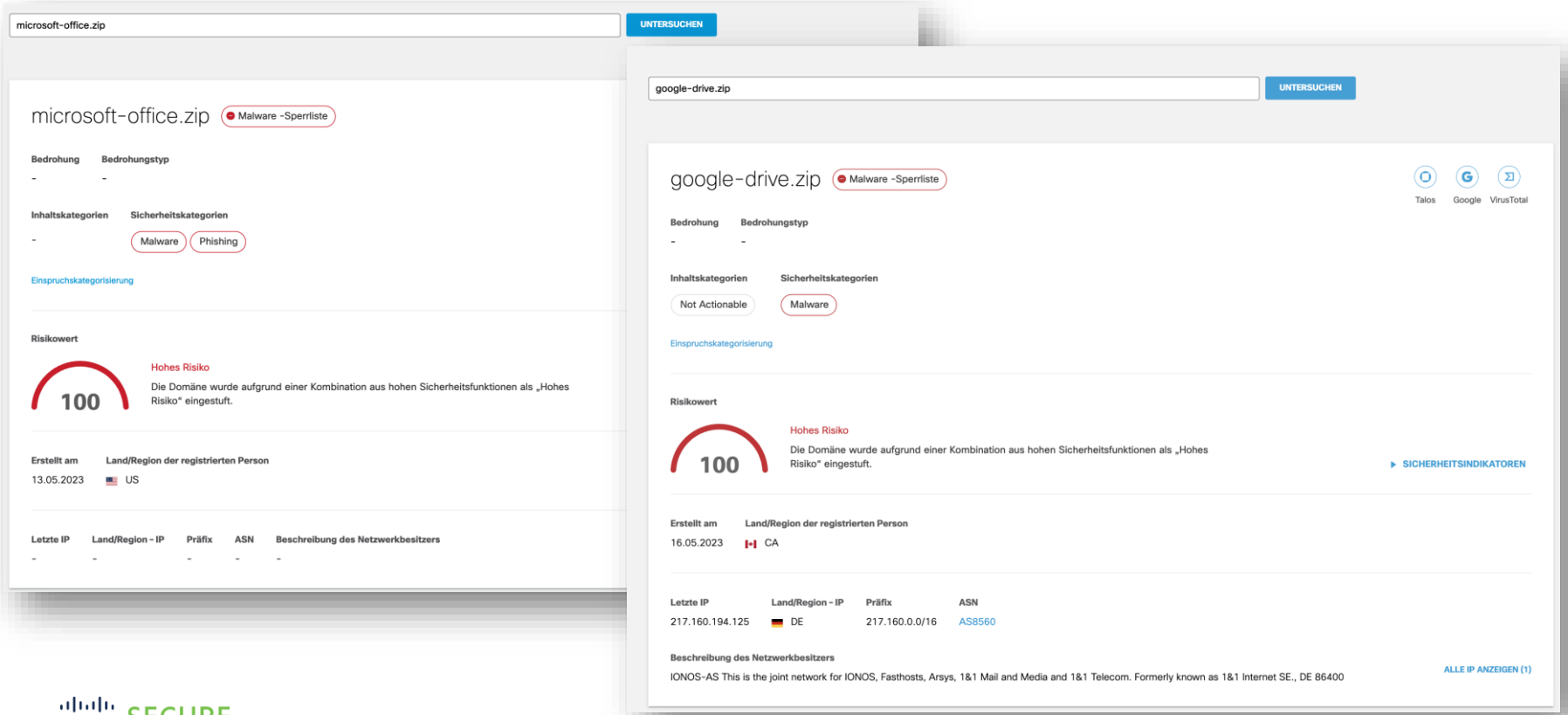
1. https://github.com/mysql/mysql-server/blob/8.0/mysql-test/std_data/data57.zip
2. https://github.com/mysql/mysql-server/blob/8.0/mysql-test/std_data/@data57.zip

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

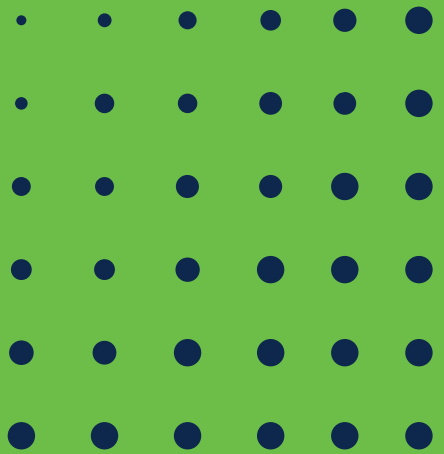
Beispiele

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

Power of Umbrella



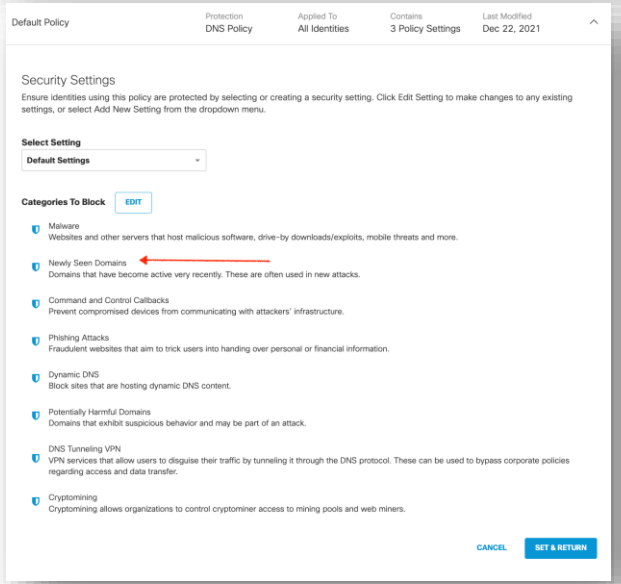
Newly Seen Domains



Newly Seen Domains

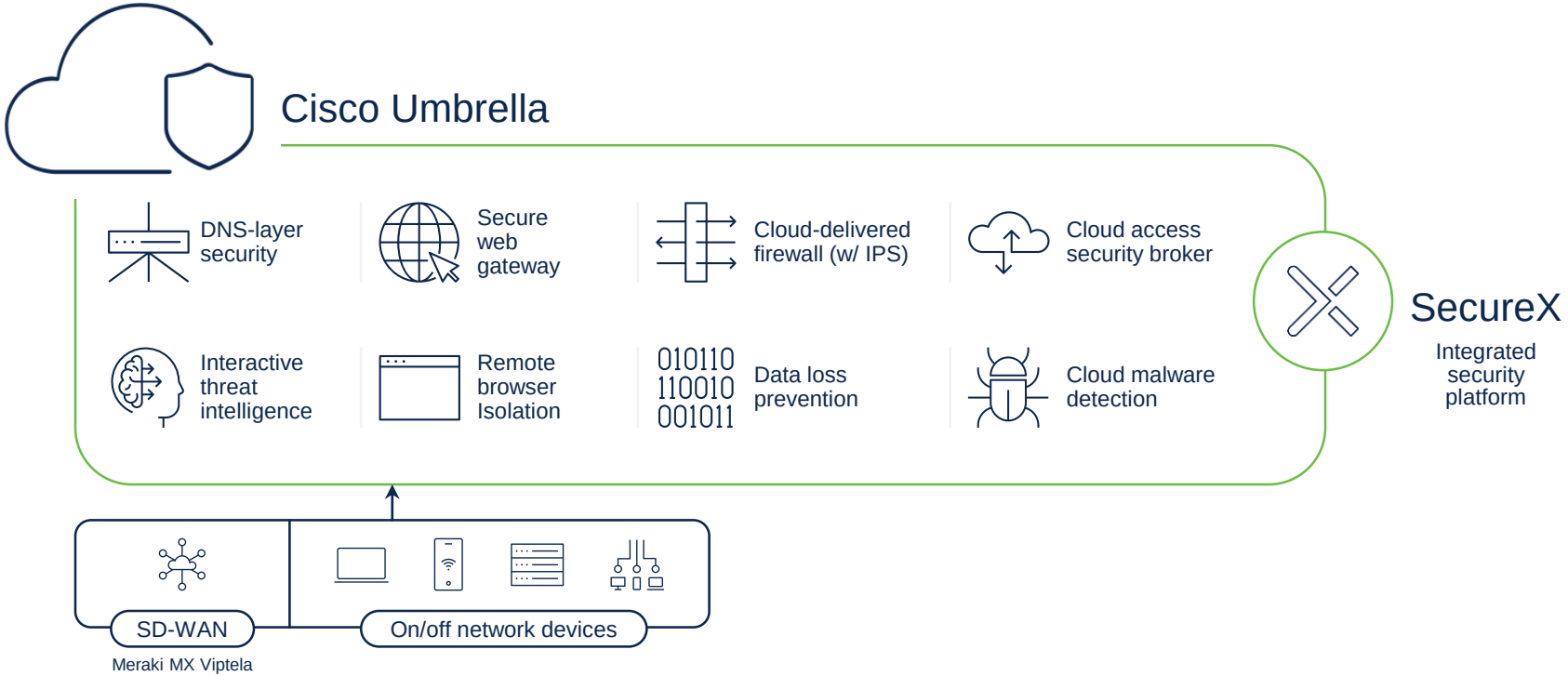
```python
def generate_domain(year: int, month: int, day: int) -> str:
    """Generate a domain name for the given date."""
    domain = ""

    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFF0) << 17)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFF8)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFE) << 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.



Cisco Umbrella

Visit our website to learn more



Demo

#fingercrossed

The bridge to possible