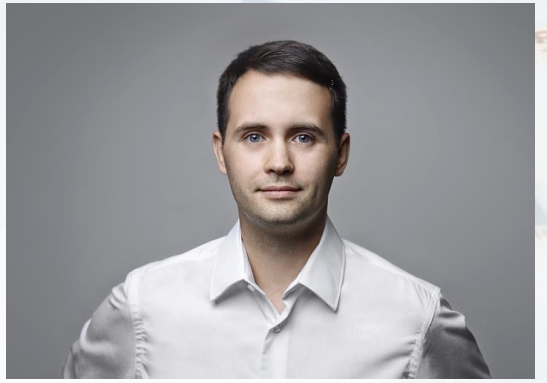
Malware als Waffe



Speaker
Maik Morgenstern
CTO
AV-TEST Institute
https://www.av-test.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Inhalt

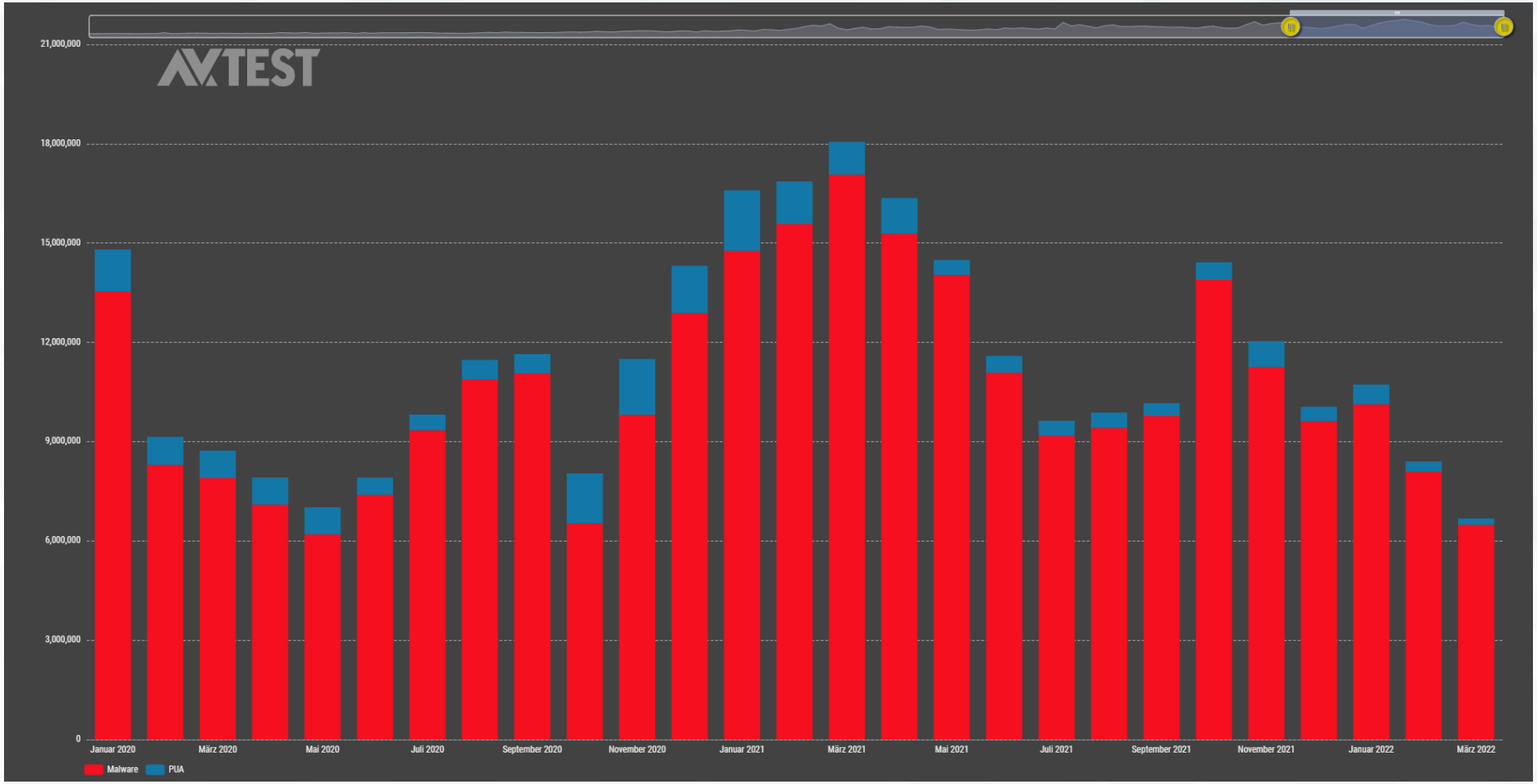
- Die Threat Landscape in den letzten drei Monaten
- Überblick über Aktivitäten gegen Ukraine
- HermeticWiper

AV-TEST

The Independent IT-Security Institute

Magdeburg Germany

Threat Landscape Q1/2022

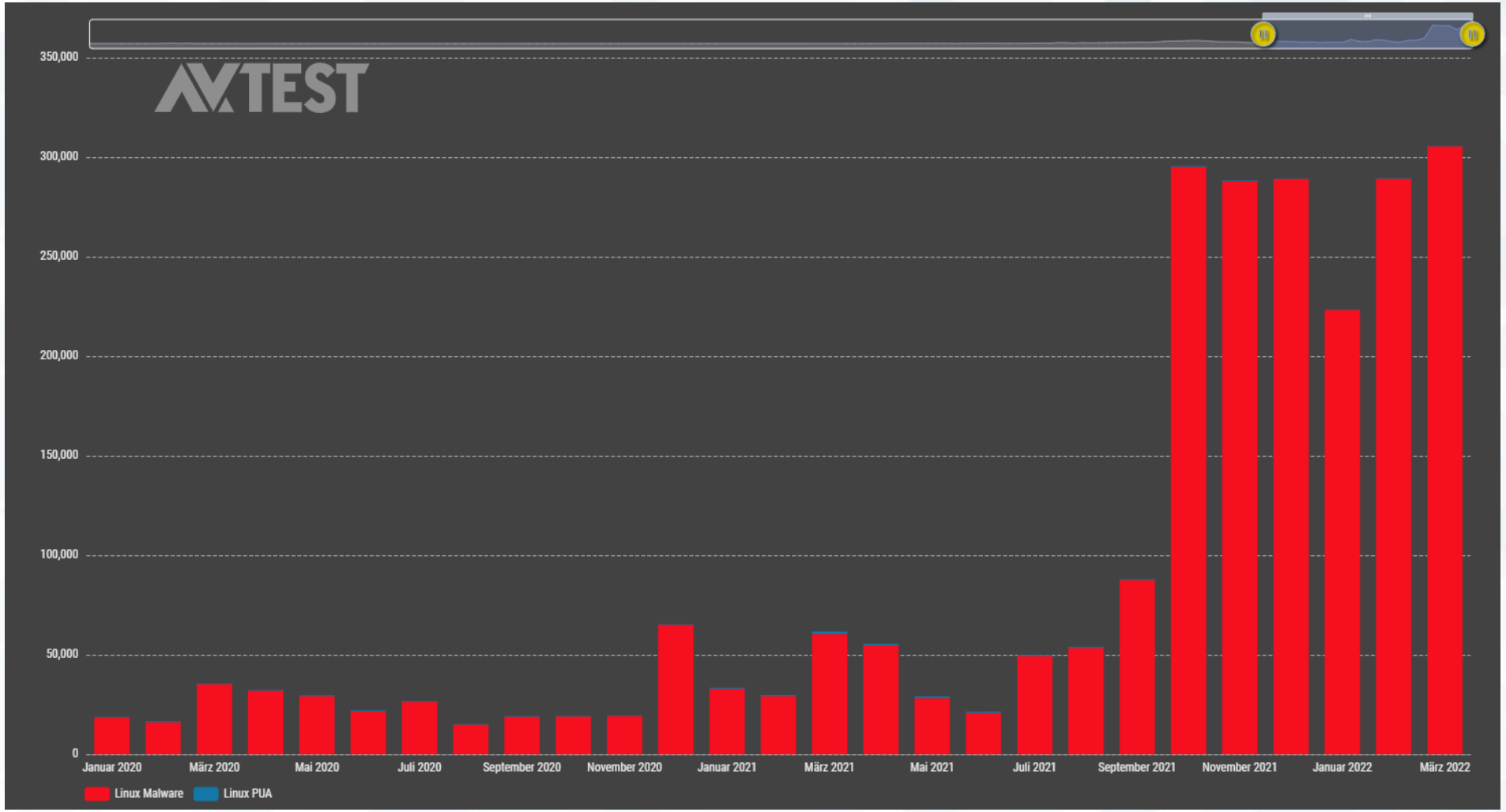


AV-TEST

The Independent IT-Security Institute

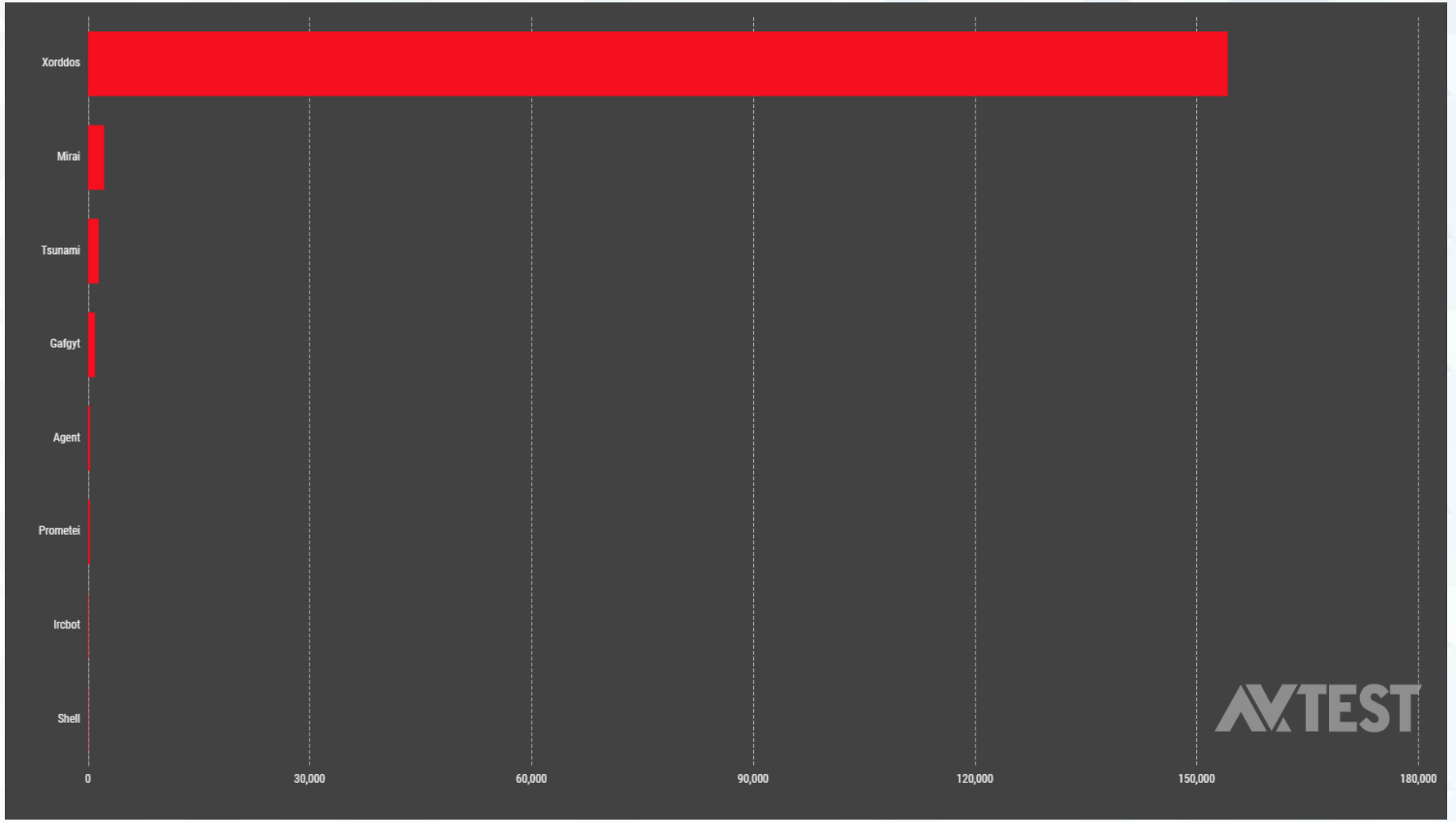
Magdeburg Germany

Threat Landscape Q1/2022 - Linux



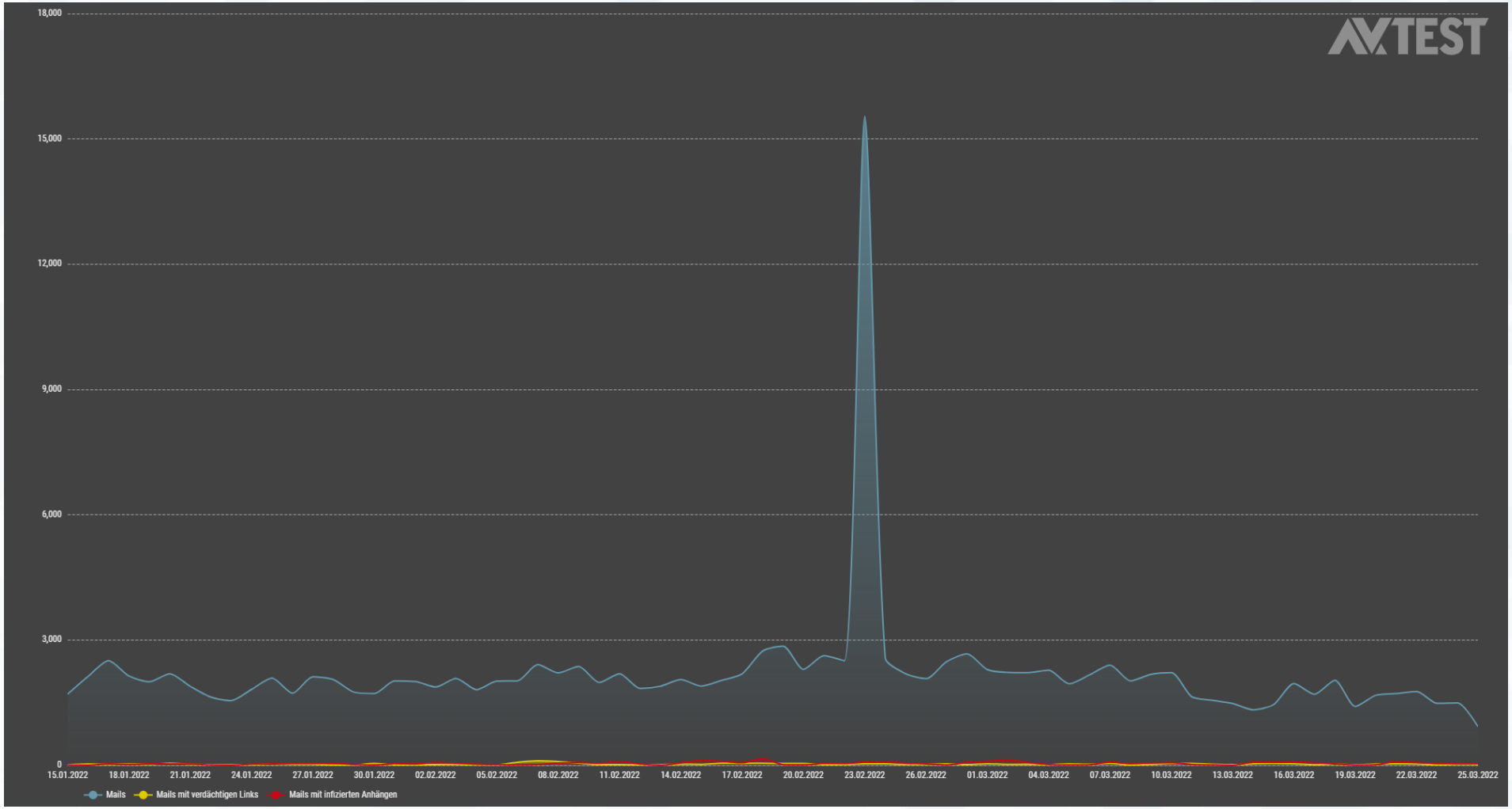
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 - Linux



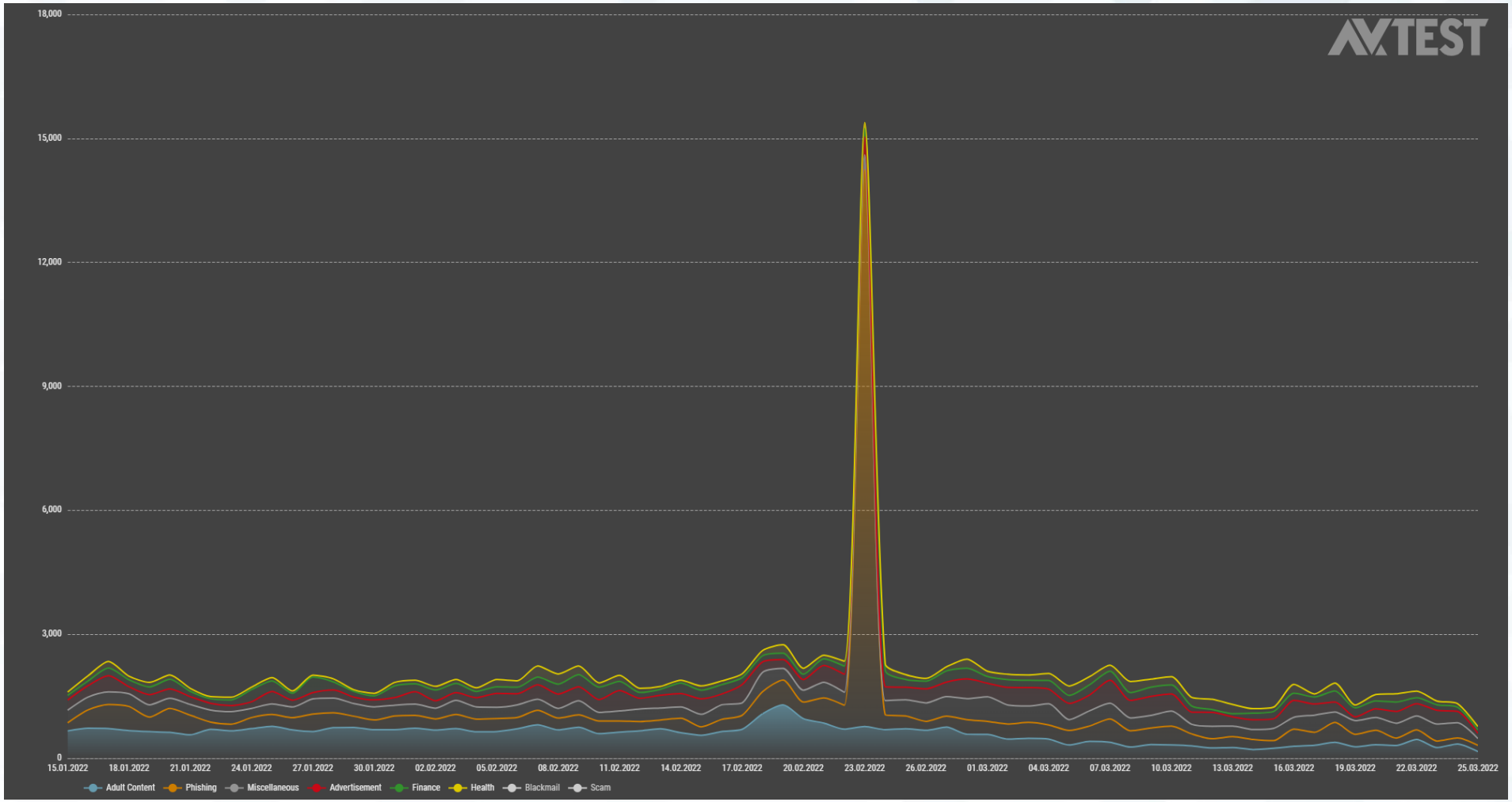
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 - Spam



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 - Spam



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 - Spam

SPAM-WELLEN

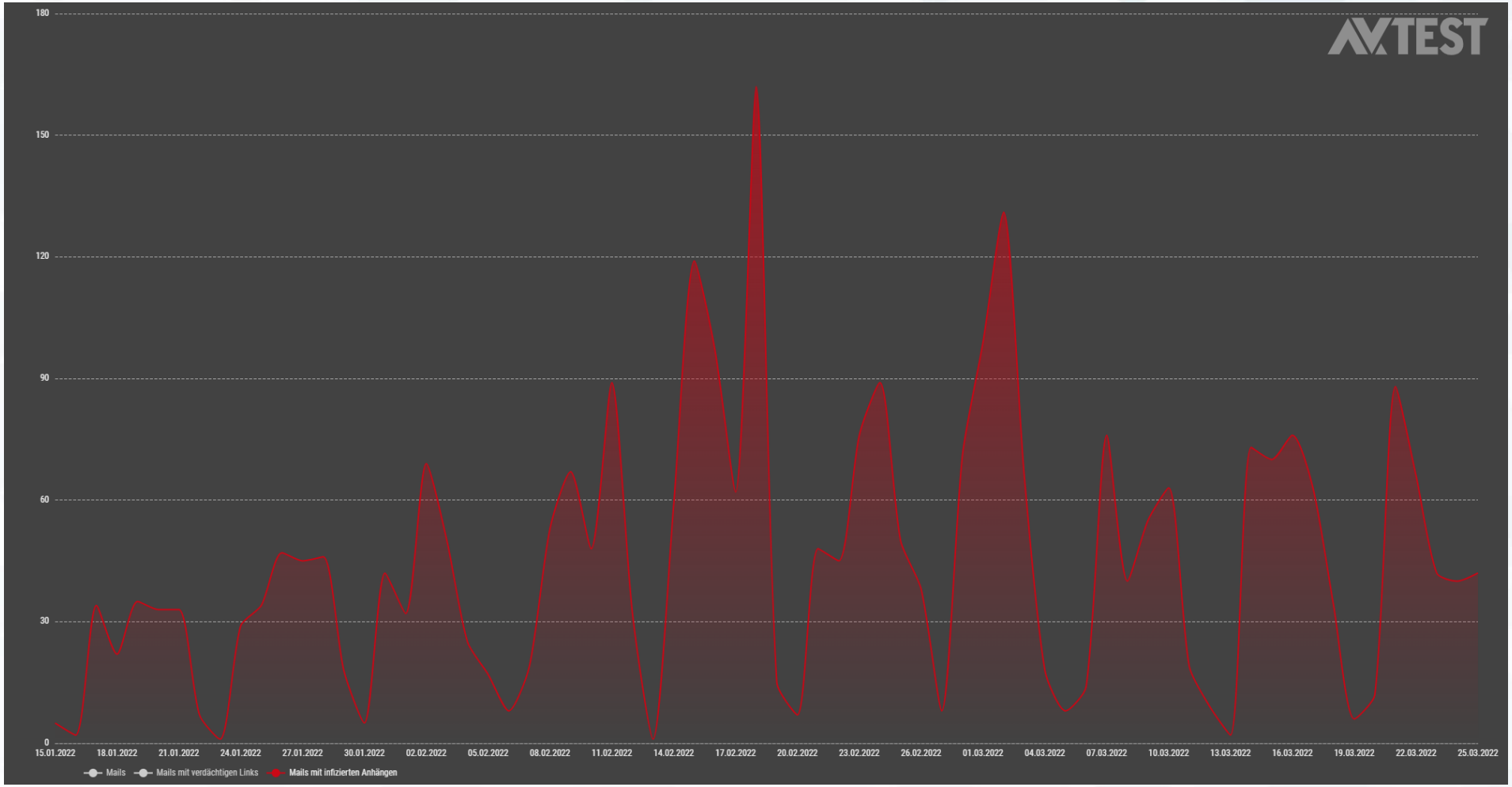
Anfang	Ende	Volumen	Weitere Merkmale
23.02.2022 10:56:26	23.02.2022 11:25:34	12,362 Mails	Betreff: DRAFTNEUE SICHERHEIT AKTIVIEREN X Mail Kategorie: Phishing Sprache: English Link Domain: vbout.com, app-n26.com, t.co, aljazeera.com Enthält Links Absender Name: NX SUPPORT NOREPLY Link URL: https://www.app-n26.com/login?_ga=2.874 https://t.co/vbsflz2s5o https://www.aljazeera.com/features/2021/2/5/melting-glaciers-rising-seas-climate-tipping-points https://www.vbout.com/?utm_source=starter&utm_medium=email-preview&utm_campaign=lemaire-autos&utm_content=powered-by https://app.vbout.com/images/vbout/powered-by-big.png Absender Domain: vbt.io Land: United States

AV-TEST

The Independent IT-Security Institute

Magdeburg Germany

Threat Landscape Q1/2022 – Malware Spam

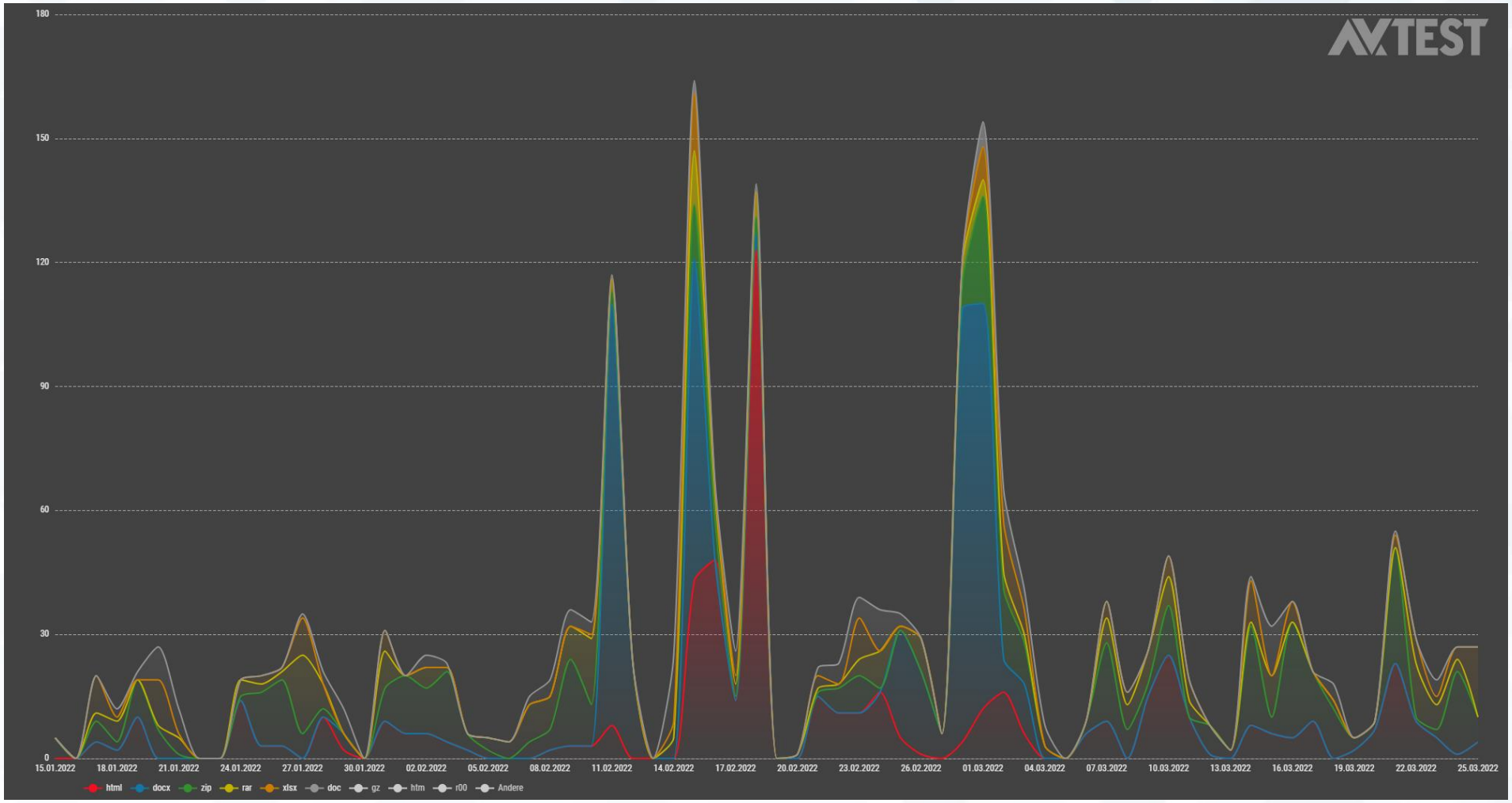


AV-TEST

The Independent IT-Security Institute

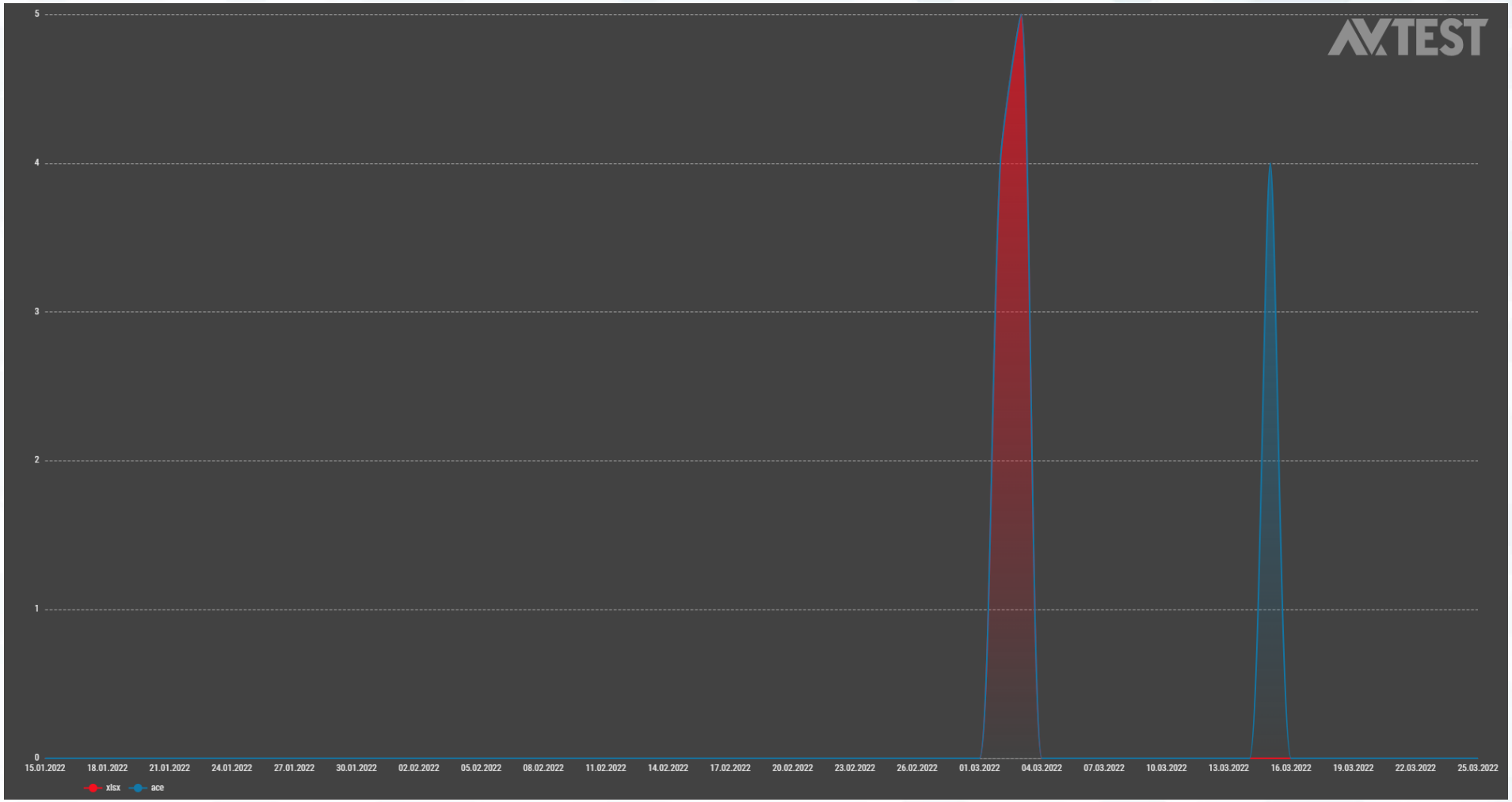
Magdeburg Germany

Threat Landscape Q1/2022 – Malware Spam



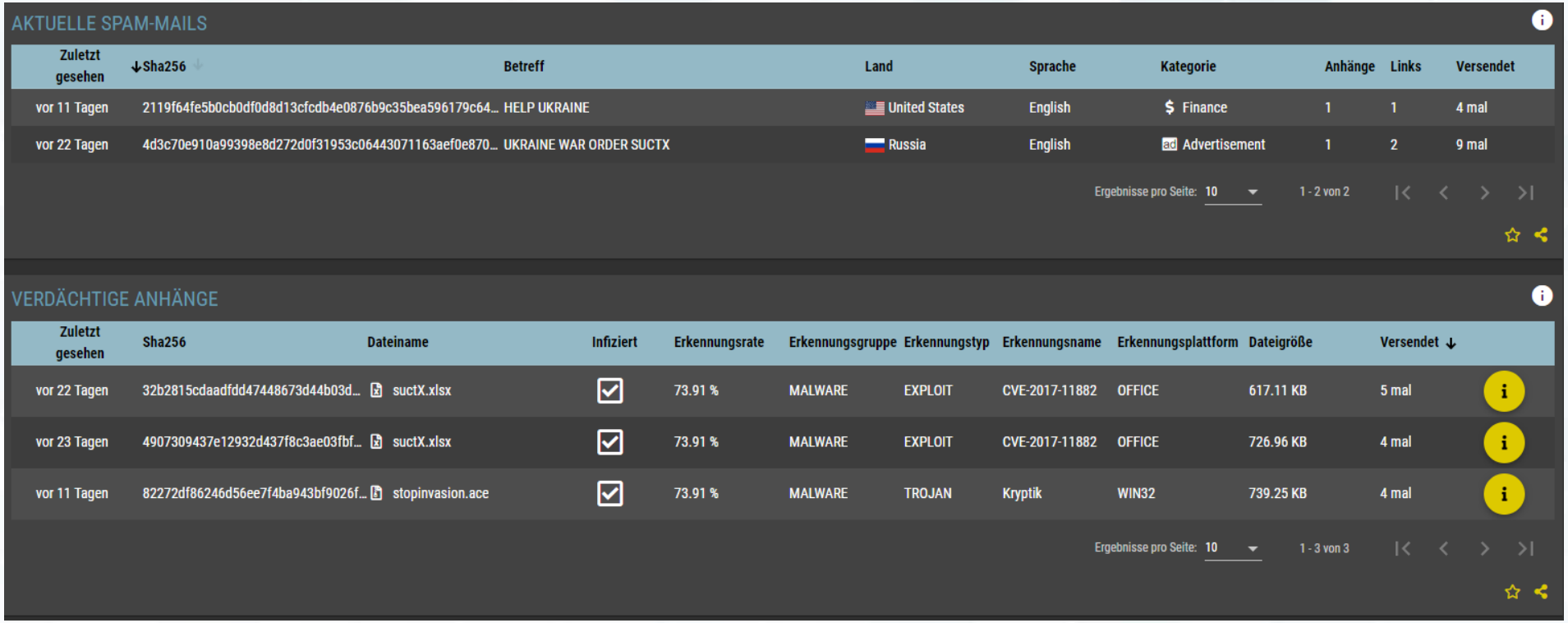
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Ukraine Malware Spam



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Ukraine Malware Spam



AKTUELLE SPAM-MAILS

Zuletzt gesehen	Sha256	Betreff	Land	Sprache	Kategorie	Anhänge	Links	Versendet
vor 11 Tagen	2119f64fe5b0cb0df0d8d13cfcdb4e0876b9c35bea596179c64...	HELP UKRAINE	United States	English	Finance	1	1	4 mal
vor 22 Tagen	4d3c70e910a99398e8d272d0f31953c06443071163aef0e870...	UKRAINE WAR ORDER SUCTX	Russia	English	Advertisement	1	2	9 mal

Ergebnisse pro Seite: 10 | 1 - 2 von 2

VERDÄCHTIGE ANHÄNGE

Zuletzt gesehen	Sha256	Dateiname	Infiziert	Erkennungsrate	Erkennungsgruppe	Erkennungstyp	Erkennungsname	Erkennungsplattform	Dateigröße	Versendet
vor 22 Tagen	32b2815cdaadfdd47448673d44b03d...	suctX.xlsx	☑	73.91 %	MALWARE	EXPLOIT	CVE-2017-11882	OFFICE	617.11 KB	5 mal
vor 23 Tagen	4907309437e12932d437f8c3ae03fbf...	suctX.xlsx	☑	73.91 %	MALWARE	EXPLOIT	CVE-2017-11882	OFFICE	726.96 KB	4 mal
vor 11 Tagen	82272df86246d56ee7f4ba943bf9026f...	stopinvasion.ace	☑	73.91 %	MALWARE	TROJAN	Kryptik	WIN32	739.25 KB	4 mal

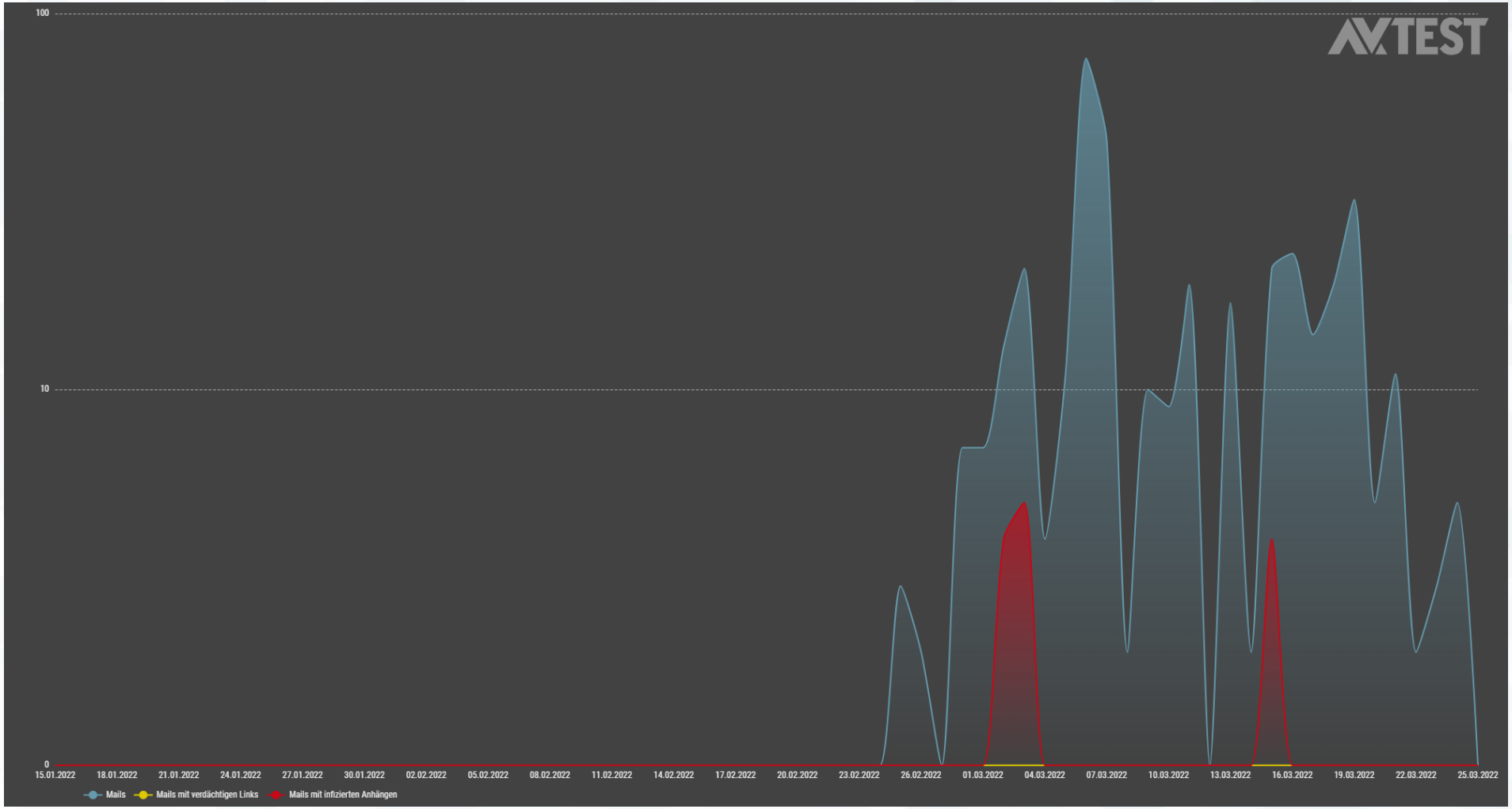
Ergebnisse pro Seite: 10 | 1 - 3 von 3

AV-TEST

The Independent IT-Security Institute

Magdeburg Germany

Threat Landscape Q1/2022 – Ukraine Scam



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Ukraine Scam

AKTUELLE SPAM-MAILS

Zuletzt gesehen	↓Sha256	Betreff	Land	Sprache	Kategorie	Anhänge	Links	Versendet
vor einem Tag	c9a5a08245b5a0dacd4a09c38d6d5e90a69994b5314663c470...	SAVE THE ORPHANS STAND WITH PEOPLE OF UKRAINE	Russia	English	Finance	1	0	15 mal
vor 2 Tagen	b822ab09137d293ff7aad925392bf2fb58dc181379a3c643a7e...	RUSSIA UKRAINE A CRY FOR HELP	Vietnam	English	Finance	1	0	4 mal
vor 2 Tagen	e9ac23029ea59aa3f8825598d9cb5a77347dc8364c17f843e6b...	HELP UKRAINE STOP THE WAR	Netherlands	English	Health	0	0	1 mal
vor 3 Tagen	cbd6ad51b5730dcb76241bf6bc96ede64eb01b2d49bc64714a...	URGENT FUND RAISING UKRAINE	Netherlands	English	Finance	2	0	1 mal
vor 4 Tagen	7d95e7c67bc678137586b85b81349aaccad36dbd7ef5c22863...	UNITED NATION MISSION FUND UKRAINE	Netherlands	English	Finance	2	0	1 mal
vor 4 Tagen	e8b06ae00da5b7309dd53338b623b2dcae75e1fcaf15c87ae16...	THREATLABZ SECURITY ADVISORY CYBERATTACKS STEMMI...	United States	English	Blackmail	0	35	1 mal
vor 4 Tagen	23e4cc501f47f7986f421b201703d0ccafa38ecb8c5b8404cf2a...	SAVE THE ORPHANS STAND WITH PEOPLE OF UKRAINE?	Russia	English	Finance	1	0	8 mal
vor 5 Tagen	814626f57fad27110ca1d6573485dcb1ee6b94b88eccdf69886...	UKRAINE TIERRETTUNG IN KRIEGSZEITEN	Germany	German	Phishing	0	32	1 mal
vor 5 Tagen	1876deed06cf2ee26024aaacd01008c00d62a0b81a11314310...	UKRAINE EMERGENCY HELP		English	Blackmail	0	0	37 mal
vor 5 Tagen	f8895fb98f1887040fbabe405c8fbad078b738ac97adb443ee0...	RUSSIA UKRAINE A CRY FOR HELP	Ireland	English	Finance	0	0	1 mal

Ergebnisse pro Seite: 10 1 - 10 von 178

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Ukraine Scam

From: info@shrind.com
Subject: **RUSSIA - UKRAINE (A CRY FOR HELP)**
To: Recipients <info@shrind.com>
Date: Tue, 08 Mar 2022 10:47:30 -0800

Good Day,

A donation campaign has been launched to support Ukraine and also help refugees fleeing the conflict in Ukraine.

We are urging you to please donate to Ukrainians as many people have fled their homes to seek refug e. Help us provide a safe solution for Ukrainian families who have already suffered too much, Shelter, water for those who need it the most in this time of crisis.

The campaign, organized by the humanitarian organization Act for Peace, is hoping to raise some fund s to support refugees in the region.

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum, USDT a nd NFT, since the banks are not working, kindly save a life, and donate to us through our UCRF (Ukrain e Crisis Relief Fund) Wallet below.

BTC- 3QzGWV38giNEpZHCh4Wa67jqKxWxhc4w1Q

Best Regards

A Cry for Help from Ukraine

Ukrainian Crisis Media Center Ukraine,
01001, Kyiv Street Khreshchatyk, 2

#Beautiful Ukraine

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Ukraine Scam

From: info@shrind.com
Subject: **RUSSIA - UKRAINE (A CRY FOR HELP)**
To: Recipients <info@shrind.com>
Date: Tue, 08 Mar 2022 10:47:30 -0800

Good Day,

Address	3QzGWV38giNEpZHCh4Wa67jqKxWxhc4w1Q
Format	BASE58 (P2SH)
Transactions	0
Total Received	0.00000000 BTC
Total Sent	0.00000000 BTC
Final Balance	0.00000000 BTC

A Cry for Help from Ukraine

Ukrainian Crisis Media Center Ukraine,
01001, Kyiv Street Khreshchatyk, 2

#Beautiful Ukraine

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Ukraine Scam

From: info@shrind.com
Subject: **RUSSIA - UKRAINE (A CRY FOR HELP)**
To: Recipients <info@shrind.com>
Date: Tue, 08 Mar 2022 10:47:30 -0800

Address	bc1qtejmtl2mtpfhq8zgaw67nwvscyfzyhq8z2qvdt
Format	BECH32 (P2WPKH)
Transactions	1
Total Received	0.00004756 BTC
Total Sent	0.00000000 BTC
Final Balance	0.00004756 BTC

Transactions

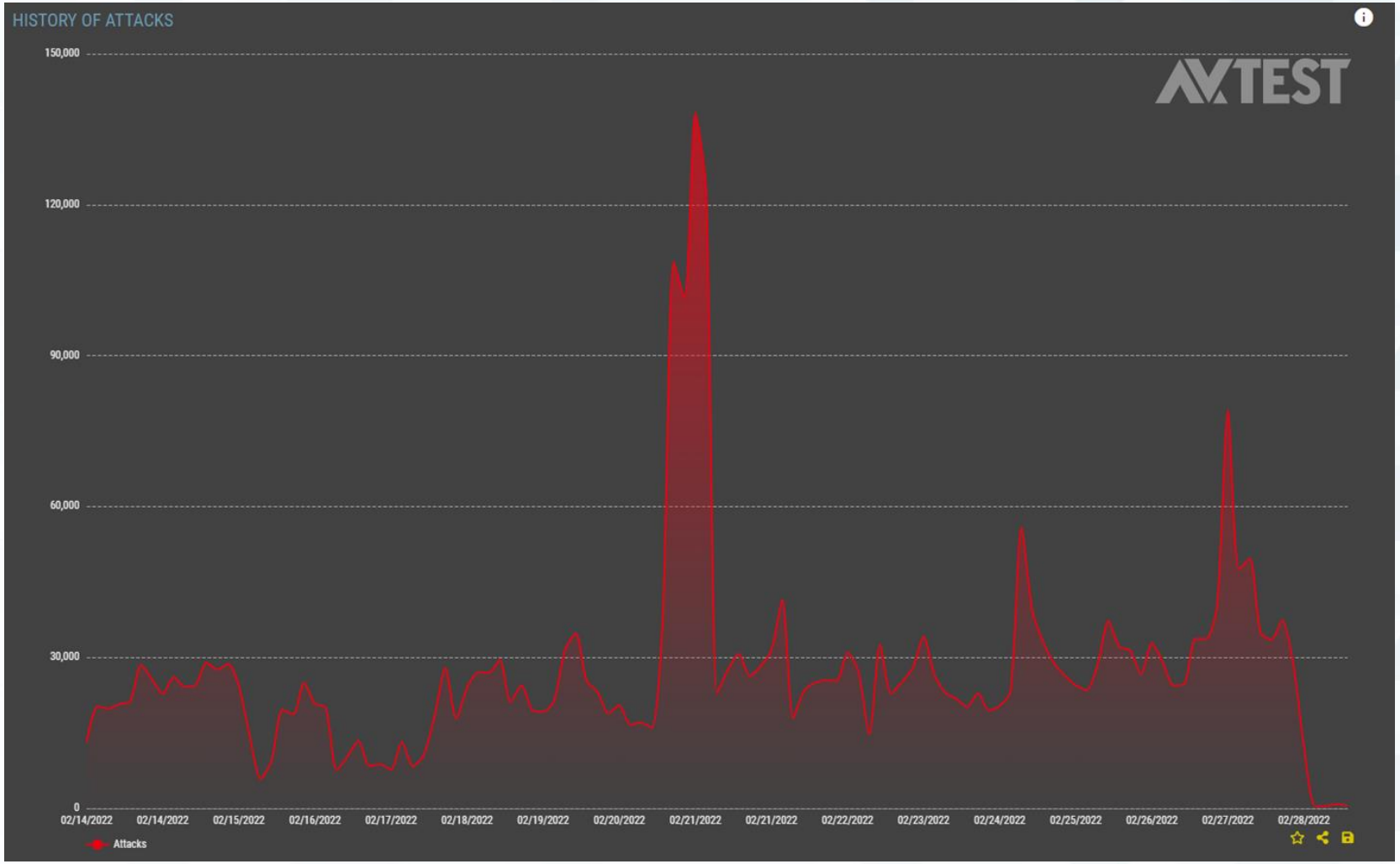
Fee	0.00000327 BTC (1.466 sat/B - 0.582 sat/WU - 223 bytes) (2.319 sat/vByte - 141 virtual bytes)			+0.00004756 BTC
Hash	df82296fd0f527de23b07f809c64f34ef3b84d9eec43a60dbd9e80d7720b95d0			2022-03-10 00:33
	bc1q3fwghmuxg25swxu6nn7c897tp6d6pp5nsthckc	0.00007838 BTC	bc1qtejmtl2mtpfhq8zgaw67nwvscyfzyhq8z2qvdt bc1q2cn59g3njsvfsjjg04qluw9fy9a0w04mktklyp	0.00004756 BTC 0.00002755 BTC

Ukrainian Crisis Media Center Ukraine,
01001, Kyiv Street Khreshchatyk, 2

#Beautiful Ukraine

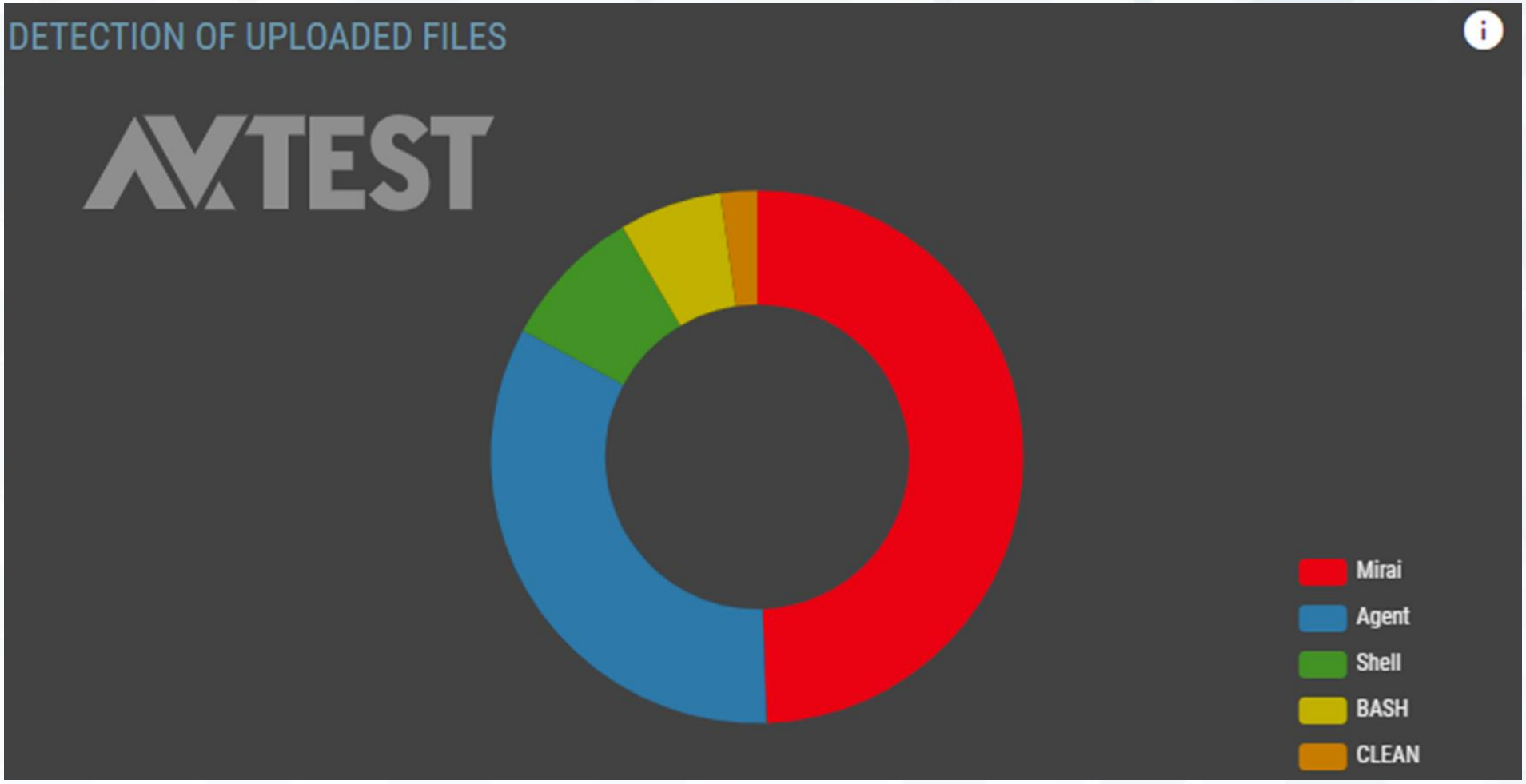
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Netzwerkangriffe



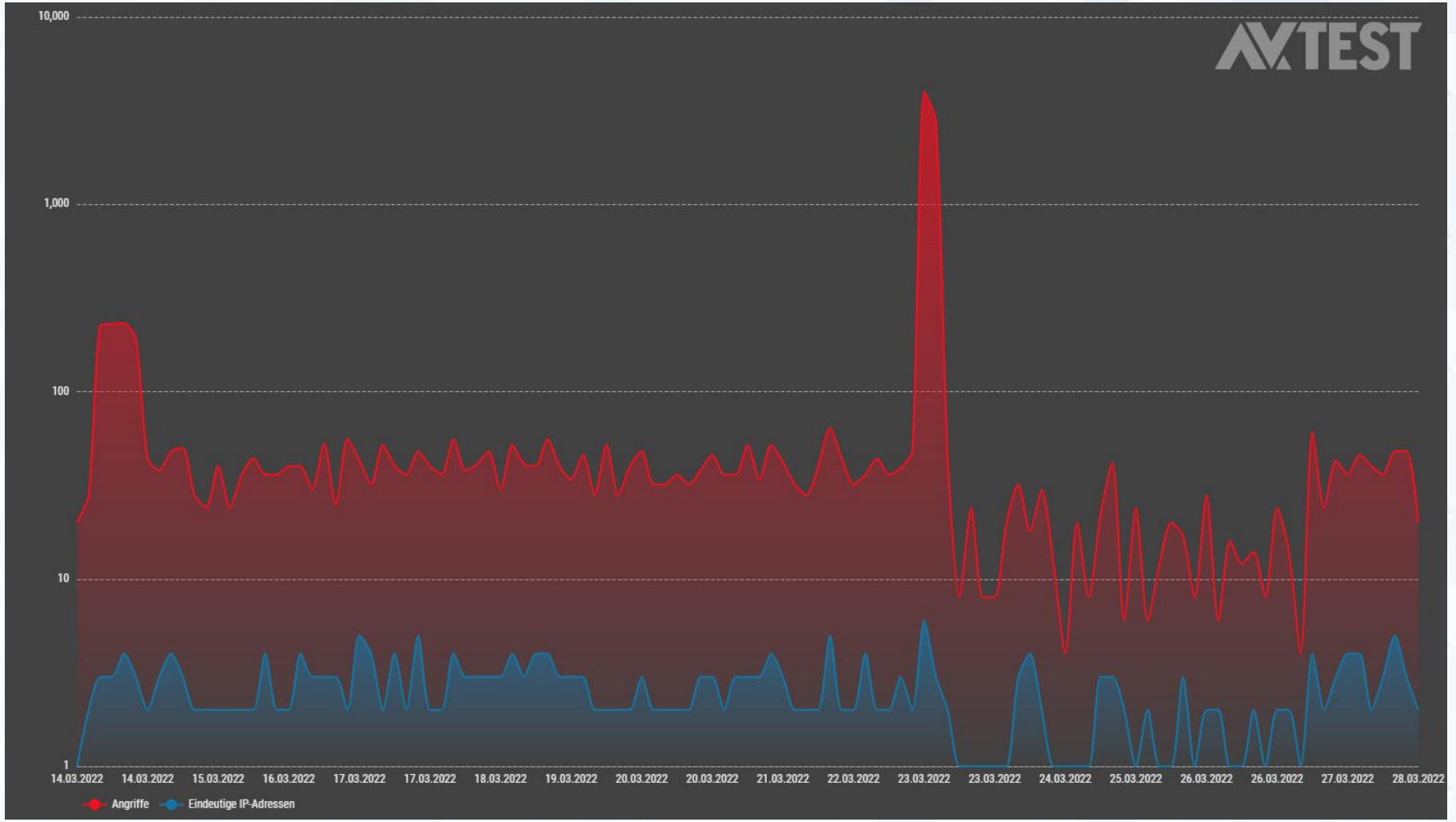
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Netzwerkangriffe



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022 – Netzwerkangriffe auf Mailserver



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Threat Landscape Q1/2022

Gesamtaktivität nicht auffällig

- Anzahl neuer Malware sogar unter dem Schnitt der Vormonate

Auffällige, kurzzeitige Änderungen im Spamaufkommen

- Um den Beginn des Krieges herum erhöhte Spamaktivität
- Änderung der eingesetzten Malware, dann schnell zurück zur „Normalität“
- Erwartbarer Scam kam schnell

Auffällige Angriffe auf Honeypots

- Ungewöhnlich starke Peaks zu Beginn des Krieges, ohne dabei auffällige Malware auszuspielen

Zeitweise und punktuell stark erhöhte Aktivität, aber insgesamt keine erhöhte Gefährdungslage ablesbar

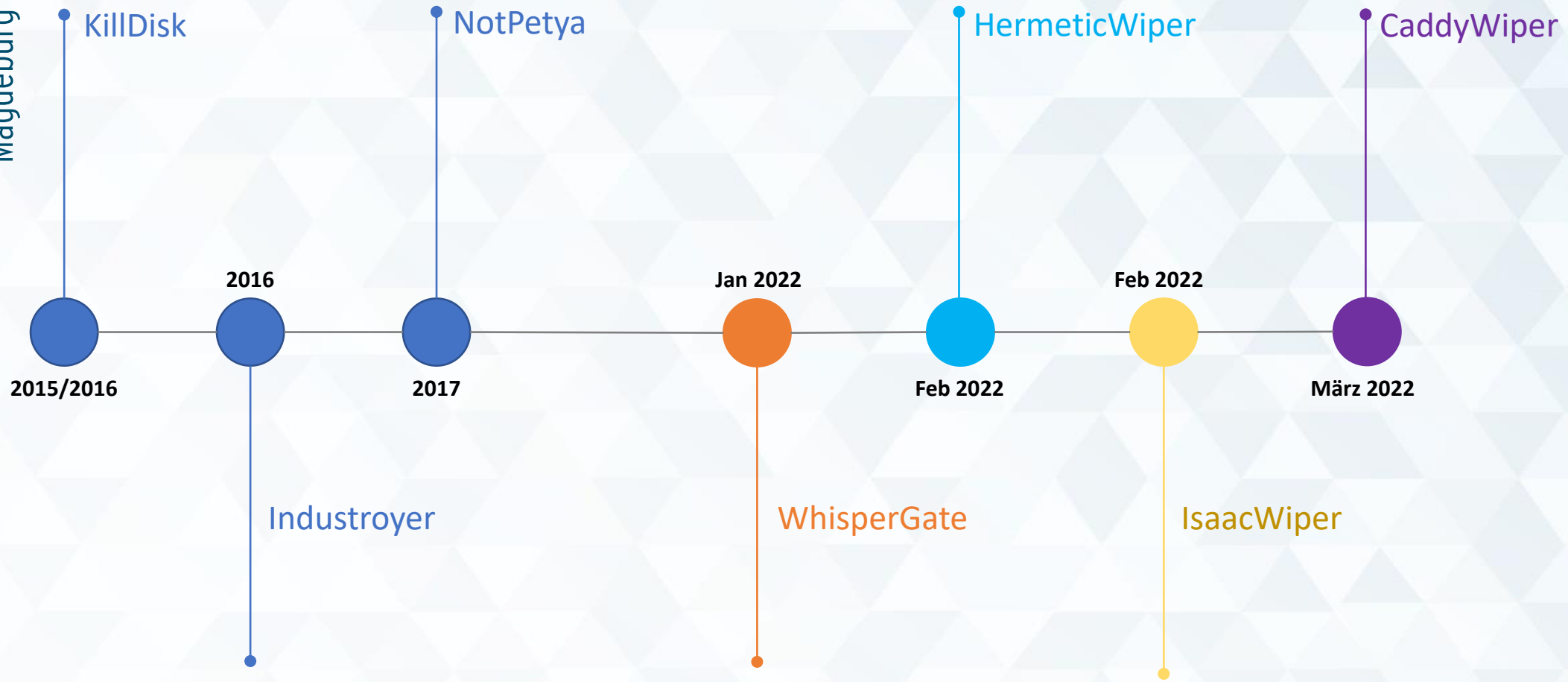
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Aktivitäten in der Ukraine

- Seit mehreren Jahren immer wieder Aktivitäten gegen Ukraine
  - Malware Angriffe insbesondere Hack and Destroy aber auch Hack and Leak → APT Group Sandworm
  - Denial of Service um Zugriff auf Webseiten und Dienste zu stören
  - Desinformationskampagnen
  - Spear Phishing Angriffe um Systeme zu kompromittieren und Zugangsdaten zu erbeuten
- U.a. vermutlich beteiligte Gruppen
  - APT28 – Fancy Bear, Sofacy
  - CyberBerkut
  - UNC1151 - Ghostwriter
  - Gamaredon
  - Sandworm - Electrum, Telebots, BlackEnergy, Voodoo Bear
  - Turla – Waterbug, WhiteBear, Snake, Krypton

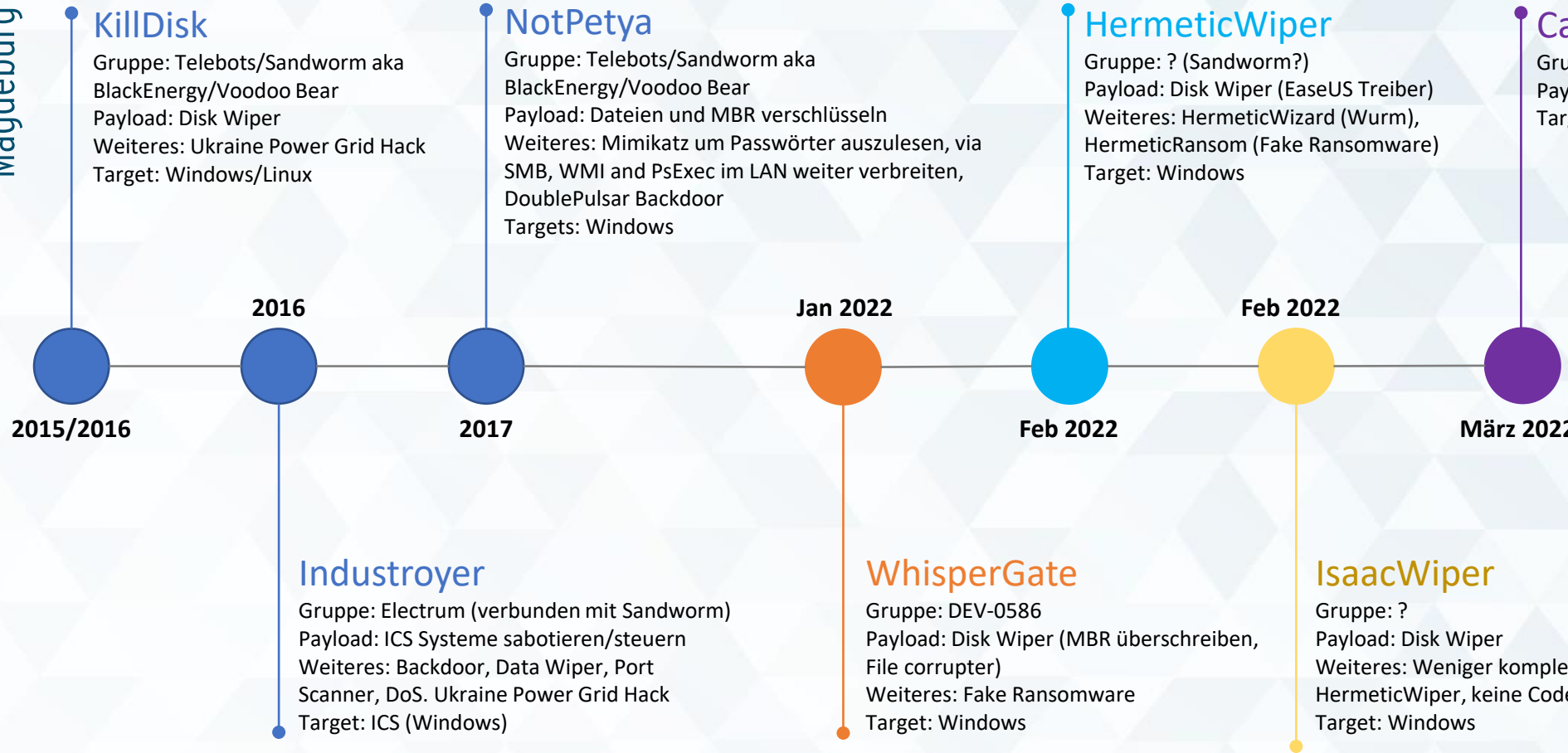
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Timeline



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Timeline

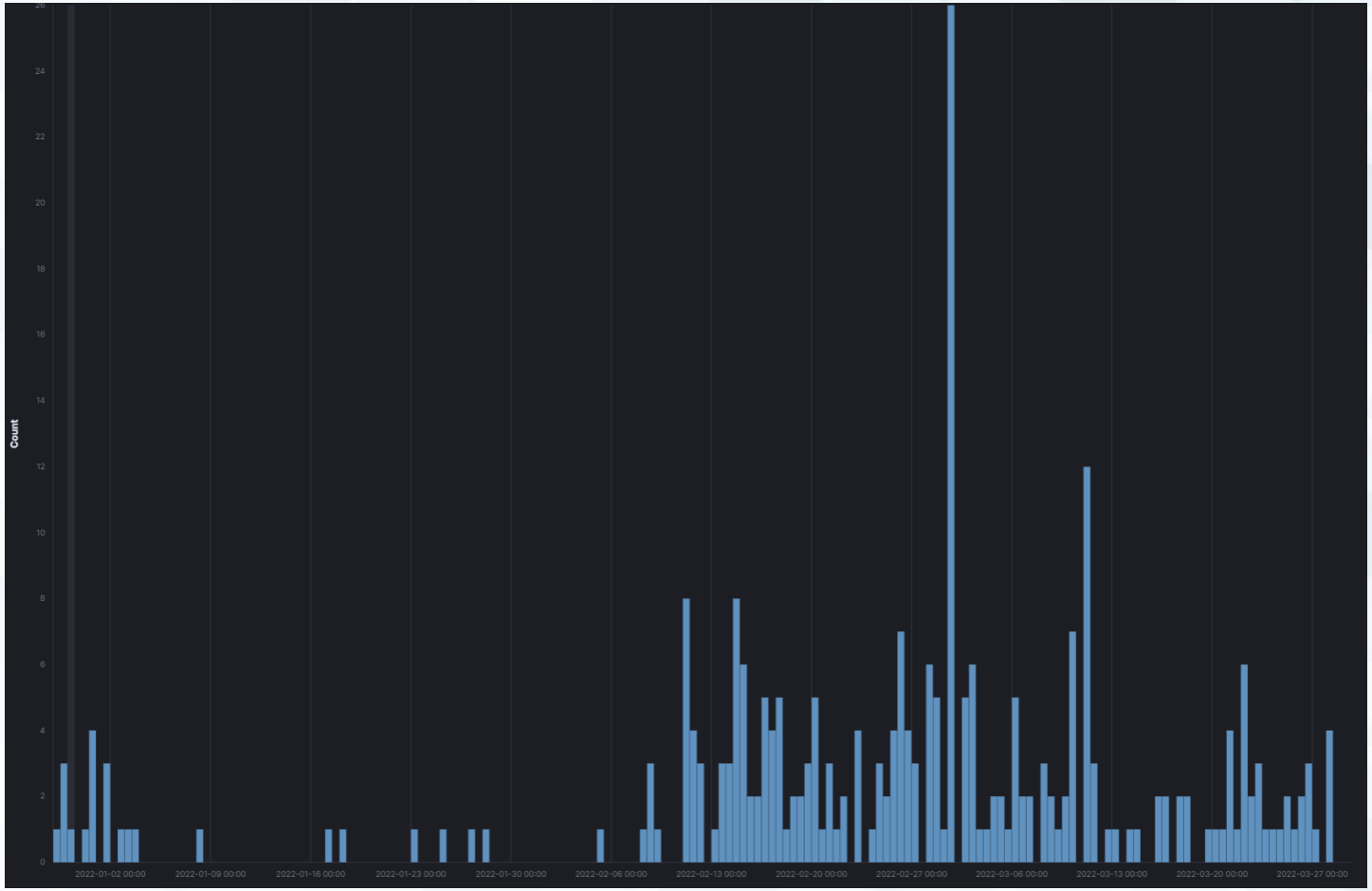


AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Timeline

Auftreten von Wiper Malware in unseren Analysen

- Beginn im Januar
- Anstieg im Februar
- Peak Ende Februar/Anfang März



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWiper

Zertifikat ausgestellt
- April 2021

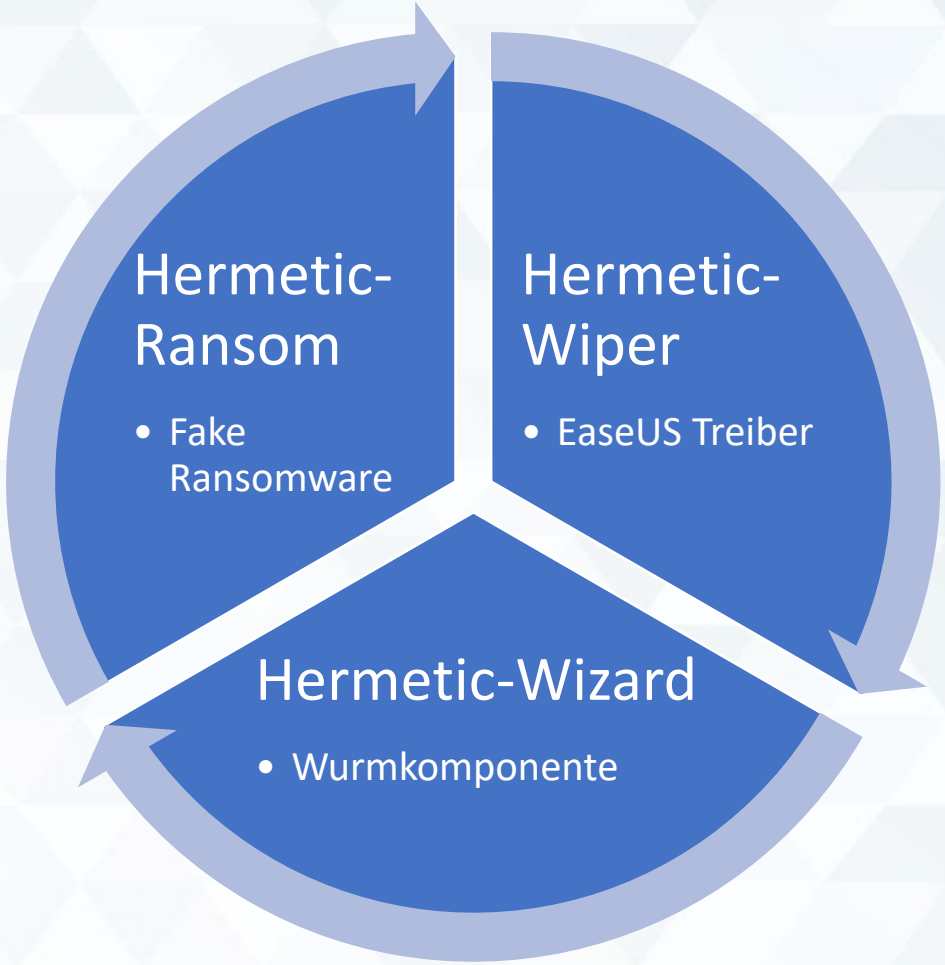
Erste HermeticWiper Datei kompiliert
- Dezember 2021

Zielsysteme infiziert (u.a. SQL und Exchange Lücken) und Zugangsdaten gestohlen
- Dezember 2021

Wiper wird verteilt und ausgeführt
- Februar 2022

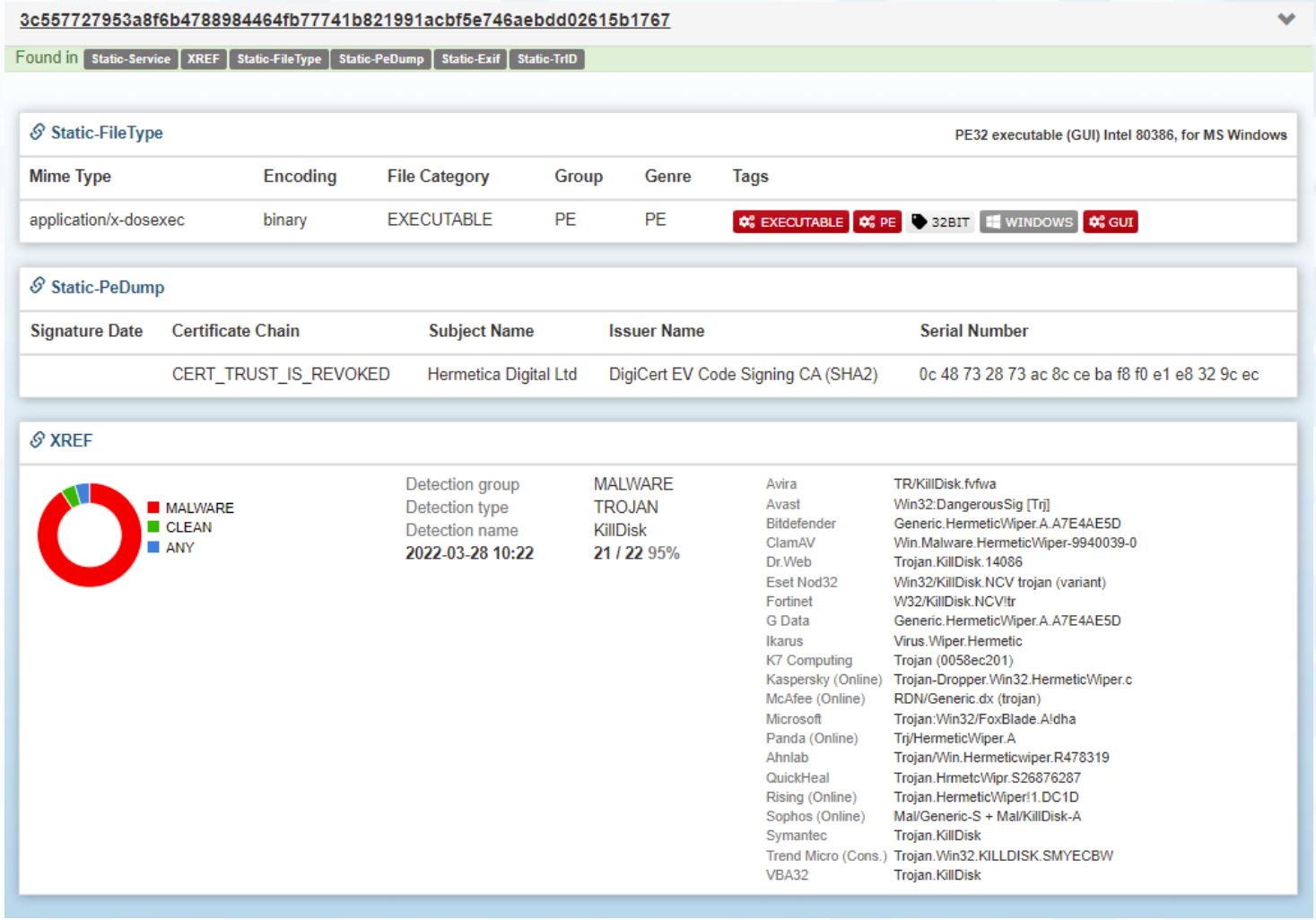
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWiper



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWiper



3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767

Found in: Static-Service | XREF | Static-FileType | Static-PeDump | Static-Exif | Static-TrID

Static-FileType — PE32 executable (GUI) Intel 80386, for MS Windows

Mime Type	Encoding	File Category	Group	Genre	Tags
application/x-dosexec	binary	EXECUTABLE	PE	PE	EXECUTABLE, PE, 32BIT, WINDOWS, GUI

Static-PeDump

Signature Date	Certificate Chain	Subject Name	Issuer Name	Serial Number
	CERT_TRUST_IS_REVOKED	Hermetica Digital Ltd	DigiCert EV Code Signing CA (SHA2)	0c 48 73 28 73 ac 8c ce ba f8 f0 e1 e8 32 9c ec

XREF

MALWARE
CLEAN
ANY

Detection group	MALWARE
Detection type	TROJAN
Detection name	KillDisk
2022-03-28 10:22	21 / 22 95%

Avira	TR/KillDisk.fvfwa
Avast	Win32:DangerousSig [Trj]
Bitdefender	Generic.HermeticWiper.A.A7E4AE5D
ClamAV	Win.Malware.HermeticWiper-9940039-0
Dr.Web	Trojan.KillDisk.14086
Eset Nod32	Win32/KillDisk.NCV trojan (variant)
Fortinet	W32/KillDisk.NCV!tr
G Data	Generic.HermeticWiper.A.A7E4AE5D
Ikarus	Virus.Wiper.Hermetic
K7 Computing	Trojan (0058ec201)
Kaspersky (Online)	Trojan-Dropper.Win32.HermeticWiper.c
McAfee (Online)	RDN/Generic.dx (trojan)
Microsoft	Trojan:Win32/FoxBlade.A!dha
Panda (Online)	Trj/HermeticWiper.A
Ahnlab	Trojan/Win.Hermeticwiper.R478319
QuickHeal	Trojan.HrmetcWipr.S26876287
Rising (Online)	Trojan.HermeticWiper!1.DC1D
Sophos (Online)	Mal/Generic-S + Mal/KillDisk-A
Symantec	Trojan.KillDisk
Trend Micro (Cons.)	Trojan.Win32.KILLDISK.SMYECBW
VBA32	Trojan.KillDisk

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWiper

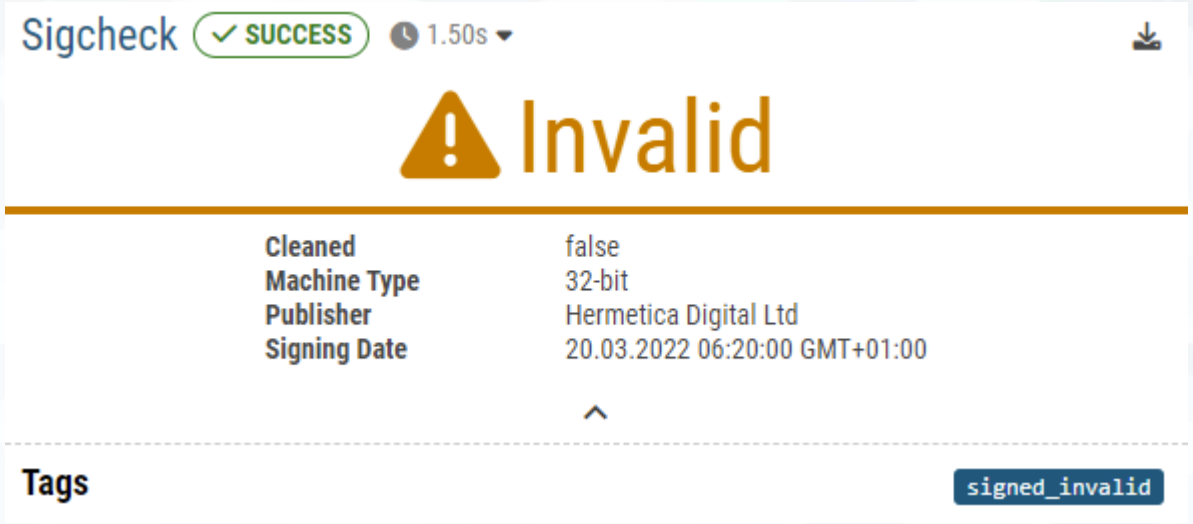
```
Certificates:
  Length:   F08
  Revision: 200
  Type:     2 (PKCS_SIGNED_DATA)

<CertificateCheck:
Verified       : SignatureNotVerified

Signer Certificate:
Serial Number  : 0c 48 73 28 73 ac 8c ce ba f8 f0 e1 e8 32 9c ec
Issuer Name    : DigiCert EV Code Signing CA (SHA2)
Subject Name   : Hermetica Digital Ltd
Revocation: The context was revoked. dwReason in pRevStatus contains the reason for revocation.

CertificateChain: CERT_TRUST_IS_REVOKED

CertificateCheck>
```



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWiper

```
BVar6 = VerifyVersionInfoW((LPOSVERSIONINFOEXW)&local_184,3,dwlConditionMask);
if (BVar6 == 0) {
  DVar11 = GetLastError();
  if (DVar11 != 0x47e) {
    return 0;
  }
  local_20 = 1;
  if (local_c == 0) {
    lpName = L"DRV_XP_X86";
  }
  else {
    lpName = L"DRV_XP_X64";
  }
}
else {
  if (local_c == 0) {
    lpName = L"DRV_X86";
  }
  else {
    lpName = L"DRV_X64";
  }
}
hResInfo = FindResourceW(DAT_00407380,lpName,L"RCDATA");
if (((hResInfo != (HRSRC)0x0) &&
    (hResData = LoadResource(DAT_00407380,hResInfo), hResData != (HGLOBAL)0x0)) &&
   (local_18 = LockResource(hResData), local_18 != (LPVOID)0x0)) {
  local_1c = (HKEY)SizeofResource(DAT_00407380,hResInfo);
```

```
<Resources (RVA: 8000)
!ResDir (0x00000000) Entries:0x03 (Named:0x01, ID:0x02) TimeDate:0x00000000
    ------------------------------------------------------------------------------
    ResDir (RCDATA) Entries:0x04 (Named:0x04, ID:0x00) TimeDate:0x00000000
        ResDir (DRV_X64) Entries:0x01 (Named:0x00, ID:0x01) TimeDate:0x00000000
            ID: 0x00000000  DataEntryOffs: 0x00000218
            DataRVA: 0x00008354  DataSize: 0x00002B6F  CodePage: 0x00000000 CRC32: 0x23D9DC32
        ResDir (DRV_X86) Entries:0x01 (Named:0x00, ID:0x01) TimeDate:0x00000000
            ID: 0x00000000  DataEntryOffs: 0x00000228
            DataRVA: 0x0000AEC4  DataSize: 0x000026B0  CodePage: 0x00000000 CRC32: 0xAAF628D2
        ResDir (DRV_XP_X64) Entries:0x01 (Named:0x00, ID:0x01) TimeDate:0x00000000
            ID: 0x00000000  DataEntryOffs: 0x00000238
            DataRVA: 0x0000D574  DataSize: 0x00002ACC  CodePage: 0x00000000 CRC32: 0x6F6104ED
        ResDir (DRV_XP_X86) Entries:0x01 (Named:0x00, ID:0x01) TimeDate:0x00000000
            ID: 0x00000000  DataEntryOffs: 0x00000248
            DataRVA: 0x00010040  DataSize: 0x0000259A  CodePage: 0x00000000 CRC32: 0xE201F370
```

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWiper

FLARE Windows SipFile

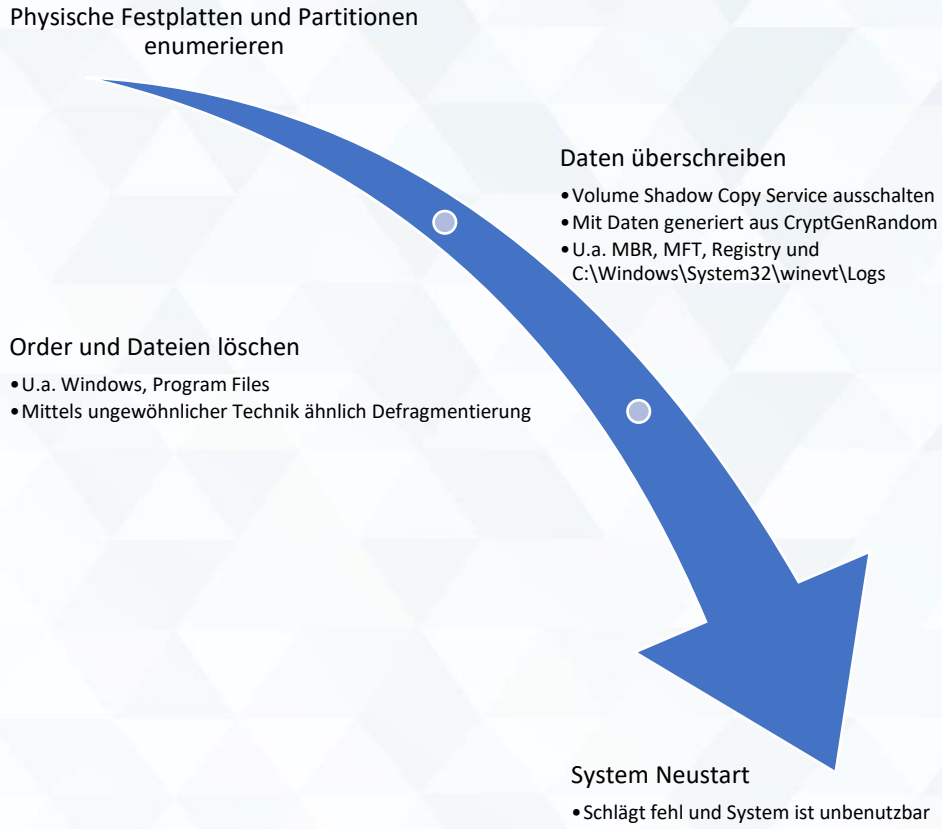
Product	Path	Name	Date
EASEUS Partition Master Server Edition 9.2.2	c:\Windows\SysWOW64\epmntdrv.sys	epmntdrv.sys	2014-03-17 15:02

FLARE Windows SipFile

Product	Path	Name	Date
EaseUS Partition Master Free Edition 10.0	c:\Program Files (x86)\EaseUS\EaseUS Partition Master 10.0\BUILDPE\x64\Windows\System32\epmntdrv.sys	epmntdrv.sys	2014-04-11 12:08

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWiper



AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticWizard

Wurmkomponente

Ebenfalls mit Hermetica Zertifikat signiert (und dadurch aufgedeckt)

Seit Februar 2022 in Ukraine aktiv

Zwei verschiedene Komponenten: DLL für SMB und DLL für WMI

Sucht sich andere Maschinen im lokalen Netzwerk

Führt dann Verbindungsversuch und Portscan durch

Versucht dann beide DLL Komponenten um sich weiter zu verbreiten

Benutzt u.a. hardcoded credentials (guest/user/root/admin und 123 oder Qaz123 als Passwort)

HermeticWizard

```
                    PTR_DAT_1004ec70                        XREF[4]:    FUN_10006e77:1000704d(R),
                                                                        FUN_1000bea0:1000bf0b(R),
                                                                        FUN_1001043c:1001052e(R),
                                                                        FUN_100113b6:10011456(R)
1004ec70 d8 e6 04 10     addr        DAT_1004e6d8
1004ec74 f8 ef 04 10     addr        DAT_1004eff8                        = 31h     1
1004ec78 00 f0 04 10     addr        u_Qaz123_1004f000                   = u"Qaz123"
1004ec7c 10 f0 04 10     addr        u_Qwerty123_1004f010                = u"Qwerty123"

                    PTR_u_guest_1004ec80                    XREF[4]:    FUN_10006e77:10007040(R),
                                                                        FUN_1000bea0:1000beea(R),
                                                                        FUN_1001043c:10010521(R),
                                                                        FUN_100113b6:1001144c(R)
1004ec80 7c ef 04 10     addr        u_guest_1004ef7c                    = u"guest"

                    PTR_u_test_1004ec84                     XREF[1]:    FUN_1000bea0:1000beea(R)
1004ec84 88 ef 04 10     addr        u_test_1004ef88                     = u"test"
1004ec88 94 ef 04 10     addr        u_admin_1004ef94                    = u"admin"
1004ec8c a0 ef 04 10     addr        u_user_1004efa0                     = u"user"
1004ec90 ac ef 04 10     addr        u_root_1004efac                     = u"root"
1004ec94 b8 ef 04 10     addr        u_administrator_1004efb8            = u"administrator"
1004ec98 d4 ef 04 10     addr        u_manager_1004efd4                  = u"manager"
1004ec9c e4 ef 04 10     addr        u_operator_1004efe4                 = u"operator"
```

```
24  int local_8;
25
26  iVar6 = 0x234;
27  if (param_1 != (char **)0x0) {
28    local_18 = inet_addr_exref;
29    local_1c = connect_exref;
30    uVar5 = 0;
31    local_24 = 1;
32    local_c = socket_exref;
33    local_20 = closesocket_exref;
34    do {
35      local_14 = 0;
36      param_1[6] = (&PTR_u_guest_1004ec80)[uVar5];
37      local_8 = 0;
38      pcVar4 = local_c;
39      do {
40        if ((short)local_24 == (short)local_8) {
41          pcVar3 = param_1[6];
42        }
43        else {
44          uVar1 = local_14 & 0xffff;
45          local_14 = local_14 + 1;
46          pcVar3 = (&PTR_DAT_1004ec70)[uVar1];
47        }
```

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticRansom

Fake Ransomware

- Gleichzeitig mit HermeticWiper verteilt, aber wesentlich geringere Verbreitung
- Auch als PartyTicket Ransomware bekannt: Ablenkung von Wiperaktivitäten

Ähnlichkeiten und Unterschiede zu HermeticWiper

- In Go statt C++ geschrieben und nicht signiert
- Aber ähnlicher Verbreitungsmechanismus, per GPO

Ungewöhnliche Textstrings in der Datei mit Bezug zur USA

- "_/C_/projects/403forBiden/wHiteHousE"
- "_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess”

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

HermeticRansom

String Search - 26 items (of 27770) - [4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382, Minimum size = 5, Align = 1]

Defined	Location	Label	Code Unit	String View
A	007072b9		ds "_/C_/projects/403forBiden/wHiteHousE"	"_/C_/projects/403forBiden/wHiteHousE"
A	005e0b90		ds "_/C_/projects/403forBiden/wHiteHousE.baggageGatherings"	"_/C_/projects/403forBiden/wHiteHousE.baggageGatherings"
A	0070730a		ds "_/C_/projects/403forBiden/wHiteHousE.baggageGatherings"	"_/C_/projects/403forBiden/wHiteHousE.baggageGatherings"
A	00749e8f		ds "_/C_/projects/403forBiden/wHiteHousE.baggageGatherings"	"_/C_/projects/403forBiden/wHiteHousE.baggageGatherings"
A	0065f042		ds "_/C_/projects/403forBiden/wHiteHousE.FileName"	"_/C_/projects/403forBiden/wHiteHousE.FileName"
A	0069659c		ds "_/C_/projects/403forBiden/wHiteHousE.FileName"	"_/C_/projects/403forBiden/wHiteHousE.FileName"
A	0072e270		ds "_/C_/projects/403forBiden/wHiteHousE.FileName"	"_/C_/projects/403forBiden/wHiteHousE.FileName"
A	005e0da8		ds "_/C_/projects/403forBiden/wHiteHousE.GoodOfficel"	"_/C_/projects/403forBiden/wHiteHousE.GoodOffice1"
A	007074c9		ds "_/C_/projects/403forBiden/wHiteHousE.GoodOfficel"	"_/C_/projects/403forBiden/wHiteHousE.GoodOffice1"
A	00749f2e		ds "_/C_/projects/403forBiden/wHiteHousE.GoodOfficel"	"_/C_/projects/403forBiden/wHiteHousE.GoodOffice1"
A	005e0e48		ds "_/C_/projects/403forBiden/wHiteHousE.init"	"_/C_/projects/403forBiden/wHiteHousE.init"
A	00707558		ds "_/C_/projects/403forBiden/wHiteHousE.init"	"_/C_/projects/403forBiden/wHiteHousE.init"
A	00749f5f		ds "_/C_/projects/403forBiden/wHiteHousE.init"	"_/C_/projects/403forBiden/wHiteHousE.init"
A	005e0c38		ds "_/C_/projects/403forBiden/wHiteHousE.lookUp"	"_/C_/projects/403forBiden/wHiteHousE.lookUp"
A	00707392		ds "_/C_/projects/403forBiden/wHiteHousE.lookUp"	"_/C_/projects/403forBiden/wHiteHousE.lookUp"
A	00749ec6		ds "_/C_/projects/403forBiden/wHiteHousE.lookUp"	"_/C_/projects/403forBiden/wHiteHousE.lookUp"
A	005e0ce0		ds "_/C_/projects/403forBiden/wHiteHousE.primaryElectionProc...	"_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess"
A	00707403		ds "_/C_/projects/403forBiden/wHiteHousE.primaryElectionProc...	"_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess"
A	00749ef2		ds "_/C_/projects/403forBiden/wHiteHousE.primaryElectionProc...	"_/C_/projects/403forBiden/wHiteHousE.primaryElectionProcess"
A	006625ab		ds "_/C_/projects/403forBiden/wHiteHousE.statictmp_0"	"_/C_/projects/403forBiden/wHiteHousE.statictmp_0"
A	0069b369		ds "_/C_/projects/403forBiden/wHiteHousE.statictmp_0"	"_/C_/projects/403forBiden/wHiteHousE.statictmp_0"
A	00730cd1		ds "_/C_/projects/403forBiden/wHiteHousE.statictmp_0"	"_/C_/projects/403forBiden/wHiteHousE.statictmp_0"
A	005e716c		ds "C:/projects/403forBiden/main.go"	"C:/projects/403forBiden/main.go"
A	0062e944		ds "C:/projects/403forBiden/main.go"	"C:/projects/403forBiden/main.go"
A	005e7475		ds "C:/projects/403forBiden/wHiteHousE/wHiteHousE.go"	"C:/projects/403forBiden/wHiteHousE/wHiteHousE.go"
A	0063deeb		ds "C:/projects/403forBiden/wHiteHousE/wHiteHousE.go"	"C:/projects/403forBiden/wHiteHousE/wHiteHousE.go"

Vielen Dank für Ihre Aufmerksamkeit!

Folgen Sie uns auf:

@avtestorg @avtestde @avatlasorg

facebook.com/avtestorg

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany