Malware Persistence versus Early Detection: AutoIT and Dridex IoC Expansion Analysis

Table of Contents

Executive Report

AutoIT-compiled malware and Dridex trace their roots to as far back as 2008 and 2014, respectively. As malware variants go, therefore, they've both had a long history and taken on various forms over time. But despite having been detected and consequently blocked with each new version, they're still alive and kicking—a testament to their persistence.

The SANS Internet Storm Center (ISC) recently reported seeing an AutoIT-compiled malware stealing information from Microsoft Outlook and Chrome. Dridex, meanwhile, resurfaced with a new entry tactic to target macOS users, according to Trend Micro. While we may not see the end of these tried-and-tested malware yet, we can attempt to mitigate the nasty repercussions they can bring with the early threat detection of suspicious Internet properties.

Armed with exhaustive WHOIS, IP, and DNS intelligence, WhoisXML API researchers expanded the lists of indicators of compromise (IoCs) identified for both threats to help users mitigate risks. Our analysis of three domains (AutoIT IoCs) and one URL (Dridex IoC) uncovered:

- Three IP addresses the AutoIT domains identified as IoCs resolved to
- 329 domains that shared the AutoIT domains' IP hosts, nine of which were deemed malicious
- 154 domains that contained the strings ***publicpress*** and ***moscowkov*** like the AutoIT IoCs
- An unredacted email address in the Dridex domain's historical WHOIS records
- 488 domains that shared the Dridex domain's registrant email address, two of which were considered malicious
- One IP address the Dridex domains resolved to
- 300 domains that shared the Dridex domain's IP host, one of which was tagged as malicious

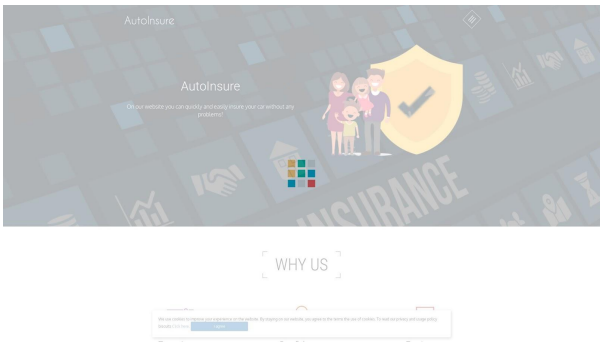
- 638 domains that contained the strings ***pr-clanky*** and ***kvalitne*** like the Dridex IoC

A Closer Look at the AutoIT-Compiled Malware IoCs

We used the three domains SANS ISC published as IoCs—publicpressmagazine[.]com, moscowkov[.]xyz, and moscowkov[.]at—for our expansion analysis for the newly discovered AutoIT-compiled malware.

First, we subjected the domains to DNS lookups, which led to the discovery of three unique IP addresses—172[.]67[.]137[.]212, 104[.]21[.]81[.]36, and 85[.]209[.]135[.]159. The first two were shared IP hosts while the last one was private. Two of the IP addresses were geolocated in the U.S. while the last one traced back to the Netherlands.

Reverse IP/DNS lookups for these IP hosts allowed us to uncover 329 possibly connected domains, 3% of which turned out to be malicious. While a majority of the malicious properties were unreachable at the time of writing, the following pages—a live auto insurance site, another that's up for sale, and an index page—may serve as malware hosts or suffer from reputation damages due to unintended links to potentially dangerous IP addresses.



Screenshot of bbbderwares[.]xyz

Screenshot of c5wult[.]cyou

Screenshot of heretopnewtopo[.]top

Next, we used two text strings—***publicpress*** and ***moscowkov***—seen among the IoCs as Domains & Subdomains Discovery search terms to find more potentially connected artifacts. That gave us 154 additional domains. While none of them are currently being detected as malicious, their resemblance to the AutoIT IoCs may make them attractive potential threat vectors for the cyber attackers' consideration.

A Deep Dive into the New Dridex Attack

Our investigation of the latest Dridex attack jumped off a URL—http://pr-clanky[.]kvalitne[.]cz/65y3fd23d/87i4g3d2d2[.]exe—identified as an IoC.

We stripped the URL down to pr-clanky[.]kvalitne[.]cz for further analysis. A historical WHOIS search for the domain name kvalitne[.]cz revealed an unredacted email address—info@webzdarma[.]cz—that we used to look for other likely connected domains. We found 488 domains, two of which—prodejce[.]cz and web2001[.]cz—were dubbed malicious.

Based on a DNS lookup, the Internet property resolved to the IP address 185[.]64[.]219[.]6, which it shared with 300 other domains, one of which—11235813[.]webzdarma[.]cz—turned out to be malicious. Note its domain's similarity with that of the unredacted email address our historical WHOIS search found. Given that the unredacted email address was used in 2017, the actors behind the old and this latest Dridex attack could be one and the same.

To gather other possible artifacts, we used two strings—***pr-clanky*** and ***kvalitne***—found in the IoC's domain as Domains & Subdomains Discovery search terms. That led to the discovery of 638 other domains. While none of them are currently being detected as malicious, their resemblance to the IoC may tempt the threat actors behind the recent Dridex attack to use them as future malware hosts.

—

Early threat detection and blocking potential attack vector access to your network is an effective means to protect against malware even those as persistent as AutoIT-compiled malware and Dridex. The identification and consequent monitoring of all possible malware entry points via an IoC list expansion can help with this process. Our in-depth investigations, for instance, added 1,425 artifacts, including 12 malicious domains, to SANS ISC's and Trend Micro's initial lists.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

AutoIT IoCs Identified by SANS ISC

- publicpressmagazine[.]com
- moscowkov[.]xyz
- moscowkov[.]at

Sample AutoIT IoC IP Resolutions

- 172[.]67[.]137[.]212
- 104[.]21[.]81[.]36

Sample AutoIT IoC IP-Connected Domains

- 25hv[.]com
- 2676999[.]com
- 2878[.]uk
- 2xbe[.]buzz
- 3commas[.]pw
- 40daysoffarming[.]com
- 4hutv[.]me
- 4m2aht[.]shop
- 4play[.]click
- 558vv[.]com
- 573y7bf[.]buzz
- 5e-shuxing[.]com
- 5egrand[.]com
- 6tq1aq[.]biz
- 7896358[.]com
- 88727120[.]com
- 918cun[.]online
- 9game[.]me
- a-great-us-senior-alarm[.]fyi
- a-great-work-from-home-intl[.]zone
- aa244[.]com
- abbubunggenre[.]tk
- abunportila[.]tk
- accarlorimathe[.]ml
- acute[.]work
- affenpocken[.]live
- afprosceyhoppartfred[.]tk
- agingparentsindependence[.]com
- agro-nav[.]ru
- aktccdeiyuhybnvr[.]ru
- al[.]liveporn[.]tv
- alaskalawenforcement[.]ml
- alelporbatttur[.]tk
- allenrajuada[.]tk
- aloutis[.]cf
- alpacatuin[.]be
- alwaysyoupermanentmakeup[.]com
- amazoneventsuae[.]com
- ammerigedi[.]gq
- andrealmenara[.]com[.]br
- angelmomsretreat[.]com
- angievargas[.]homes
- anlefrifor[.]tk
- anzinkabubo[.]tk
- api[.]9game[.]me
- api[.]darkswap[.]finance
- applausr[.]net
- apple-technology[.]com
- appzdl[.]com
- aqiqijnb[.]ml

Sample Malicious AutoIT IoC IP-Connected Domains

- bbbderwares[.]xyz
- boydsbayenvironmental[.]com[.]au

- c5wult[.]cyou
- heretopnewtopo[.]top
- heylotmeort[.]top

Sample AutoIT IoC String-Connected Domains

- publicpress[.]us
- publicpress[.]vg
- publicpress[.]hu
- publicpress[.]tk
- publicpress[.]pl
- publicpress[.]dk
- publicpress[.]co
- publicpress[.]in
- publicpress[.]jp
- publicpress[.]me
- publicpress[.]de
- publicpress[.]com
- publicpress[.]org
- publicpress[.]net
- publicpress[.]biz
- publicpress[.]xyz
- republicpress[.]in
- publicpress[.]live
- publicpresse[.]net
- publicpressny[.]ga

Dridex IoC Identified by Trend Micro

- pr-clanky[.]kvalitne[.]cz

Sample Dridex IoC Email-Connected Domains

- dekorativne-stierky[.]sk
- cryosoft[.]sk
- speedminton-b2b[.]sk
- wz[.]sk
- meteofilakovo[.]sk
- autooobazar[.]sk
- ticketexchange[.]sk
- gemerflora[.]sk
- revoltmedia[.]sk
- kandidatnastarostu[.]sk
- herbushka[.]sk
- dentkat[.]sk
- pocinote[.]sk
- alibang[.]sk
- be-free[.]sk
- ezatcaffee[.]sk
- samkonm[.]sk
- dirtkillers[.]sk
- karmenncare[.]cz
- jakubmarecek[.]cz
- vmodels[.]cz
- kadernictvikocka[.]cz
- kolanovyjicin[.]cz
- veronica-club[.]cz
- johnnyvonbahnhof[.]cz
- novak-instalater[.]cz
- humans-era[.]cz
- minigolfista[.]cz
- pizzerienaohrade[.]cz
- tempemjobs[.]cz
- nocnivlak[.]cz
- njdesign[.]cz
- wzp[.]cz
- tefl[.]cz
- zaloznizdroje[.]cz
- svjslepahoblikova[.]cz
- webnaprani[.]cz
- wfdataservis[.]cz
- portretistka[.]cz
- svatyjakub[.]cz

- moravskyadrenalin[.]cz
- zahradaoda[.]cz
- pepinocomputers[.]cz
- svsh405[.]cz
- sdhsendrazice[.]cz
- mjirkovareality[.]cz
- zemekf[.]cz
- mbbagr[.]cz
- moraviaspider[.]cz
- mks-trading[.]cz

Sample Malicious Dridex IoC Email-Connected Domain

- prodejce[.]cz

Dridex IoC IP Resolution

- 185[.]64[.]219[.]6

Sample Dridex IoC IP-Connected Domains

- 0tam[.]eu
- 1-sustanon[.]wz[.]cz
- 1[.]crossminton[.]sk
- 11235813[.]webzdarma[.]cz
- 1stdesign[.]kvalitne[.]cz
- 2014-2[.]euweb[.]cz
- 2014-3[.]euweb[.]cz
- 234realnavirtualita[.]wz[.]sk
- 24-eon[.]cz
- 2pacweb[.]wz[.]cz
- 384[.]cz
- 3dnamiru[.]cz
- 3draven[.]com
- 3najednou[.]cz
- 4473243uk47328493289[.]com
- 4acords[.]webz[.]cz
- 4gkh[.]wz[.]cz
- 4k[.]wz[.]cz
- 6zstrinec[.]wz[.]cz
- 7ngay[.]cz
- 9bmelnik[.]cz
- a40[.]wz[.]cz
- abapartments[.]wz[.]cz
- abdinsula[.]mysteria[.]cz
- abhsia[.]buchl[.]cz
- abieskriz[.]cz
- abigail[.]unas[.]cz
- ac[.]crossminton[.]sk
- acaboczech[.]cz
- ad-soltys[.]cz
- adam-skrabanek[.]webzdarma[.]cz
- adamplanet[.]cz
- adapchmelar[.]eu
- adelasos[.]cz
- administration[.]crossminton[.]sk
- adr-poradce[.]cz
- adrenalinovecentrum[.]cz
- adrspach[.]wz[.]cz
- ads[.]buchl[.]cz
- adsl[.]buchl[.]cz
- aerobik[.]wz[.]cz
- aeternias[.]cz
- afamos[.]cz
- affiliate[.]wz[.]sk
- affiliates[.]buchl[.]cz
- agasil[.]cz
- agentura52[.]com
- agilityudoli[.]cz
- agrobazarmartinek[.]wz[.]cz

Malicious Dridex IoC IP-Connected Domain

- 11235813[.]webzdarma[.]cz

Sample Dridex IoC String-Connected Domains

- pr-clanky[.]sk
- pr-clanky[.]eu
- pr-clanky[.]cz
- pr-clanky[.]com
- pr-clanky[.]net
- pr-clanky[.]info
- seo-pr-clanky[.]cz
- pr-clanky-ihned[.]cz
- profi-pr-clanky[.]sk
- pr-clanky-zdarma[.]cz
- kvalitni-pr-clanky[.]cz
- reklamni-pr-clanky[.]net
- kvalitni-pr-clanky[.]net
- kvalitne[.]pw
- kvalitne[.]cz
- kvalitne[.]eu
- kvalitne[.]sk
- ikvalitne[.]cz
- kvalitne[.]net
- kvalitne[.]com
- nekvalitne[.]cz
- cvkvalitne[.]cz
- pckvalitne[.]cz
- rdkvalitne[.]cz
- mpkvalitne[.]cz
- kvalitneji[.]cz
- kvalitne[.]info
- kvalitnezit[.]cz
- kvalitnebpr[.]sk
- zijkvalitne[.]cz
- kvalitnejsi[.]cz
- snykvalitne[.]cz
- alukvalitne[.]cz
- webkvalitne[.]cz
- seokvalitne[.]sk
- jenkvalitne[.]cz
- lpgkvalitne[.]cz
- kvalitneseo[.]cz
- kvalitneule[.]sk
- pc-kvalitne[.]cz
- seokvalitne[.]cz
- fitkvalitne[.]cz
- nekvalitne[.]xyz
- kvalitneled[.]sk
- domkvalitne[.]sk
- webkvalitne[.]eu
- kvalitnecbd[.]eu
- kvalitnecbd[.]sk
- autokvalitne[.]cz
- brnokvalitne[.]cz
- pneukvalitne[.]sk
- kvalitnevino[.]sk
- kvalitnepivo[.]sk
- domykvalitne[.]cz
- kvalitne[.]online
- kvalitnevina[.]sk
- danekvalitne[.]cz
- pneukvalitne[.]cz
- seo-kvalitne[.]cz
- kvalitnenoze[.]sk
- kvalitneokna[.]sk
- kvalitnedata[.]sk
- kvalitneweby[.]eu
- gdprkvalitne[.]cz
- motokvalitne[.]cz
- kvalitneveci[.]eu
- tlackvalitne[.]sk
- webykvalitne[.]cz

- uctokvalitne[.]cz
- kvalitnekoze[.]sk
- spimkvalitne[.]cz
- motokvalitne[.]sk
- obuvkvalitne[.]cz
- kvalitnenoze[.]eu
- kvalitne-seo[.]cz
- kvalitneokna[.]eu
- tiskkvalitne[.]cz
- vinokvalitne[.]cz
- kvalitneauta[.]sk
- kvalitnerumy[.]sk
- kvalitneveci[.]sk
- kvalitnemaso[.]sk
- kvalitnebyty[.]sk
- oknakvalitne[.]cz
- kvalitne-sit[.]eu
- bozpkvalitne[.]cz
- kvalitneweby[.]sk
- kvalitnedomy[.]sk
- kvalitnebudy[.]sk
- kvalitnepneu[.]sk
- rybykvalitne[.]cz
- kvalitnefoto[.]sk
- web-kvalitne[.]cz
- lokokvalitne[.]ws
- kupujkvalitne[.]cz
- domy-kvalitne[.]cz
- kvalitneploty[.]sk
- brylekvalitne[.]cz
- kurzykvalitne[.]cz
- kvalitnekable[.]sk