頑固なマルウェアを早期発見：AutoITとDridexのIoCリストを拡充

目次

要旨

AutoITでコンパイルされたマルウェアとDridexの起源は、それぞれ2008年と2014年にまでさかのぼります。そして、どちらも時間と共に様々な形に変化してきました。新たなバージョンになるたびに検出、ブロックされてもしぶとく生き残り、今も健在です。

SANS Internet Storm Center（ISC）が最近、AutoITでコンパイルされたマルウェアがMicrosoft OutlookとChromeから情報を盗み出すのを目撃した、との報告を出しました。他方、Trend Microによると、macOSユーザーを狙う新たな侵入手口としてDridexが再び姿を現したとのことです。多くの試練を生き延びてきたこのようなマルウェアがなくなることはないかもしれません。しかし、不審なインターネットのプロパティを早期に検知することで、マルウェアがもたらす厄介な影響を軽減することは可能です。

そこで、WhoisXML APIでは、WHOIS、IPアドレスおよびDNSの幅広いインテリジェンスを駆使し、上の2種類の脅威に関連して特定されたIoC（セキュリティ侵害インジケーター）のリストをさらに拡充しました。具体的には、当社で3つのドメイン名（AutoIT IoC）と1つのURL（Dridex IoC）を分析した結果、以下を発見しました。

- AutoIT IoCとされたドメイン名が名前解決した3つのIPアドレス
- AutoITのドメインと同じIPアドレスを使っている329個のドメイン名。うち9個は悪意があると判定
- AutoIT IoCと同様に「publicpress」と「moscowkov」という文字列を含む154個のドメイン
- Dridexのドメイン名の過去の WHOIS レコードに表示された無編集のメールアドレス1件
- Dridexのドメイン名と同じ登録者メールアドレスを持つドメイン名が488個。うち2つは悪意あるものと判明
- Dridexのドメイン名が名前解決した1つのIPアドレス
- Dridexのドメイン名と同じIPアドレスを使用している300個のドメイン名。うち1つは悪意あるものと判明

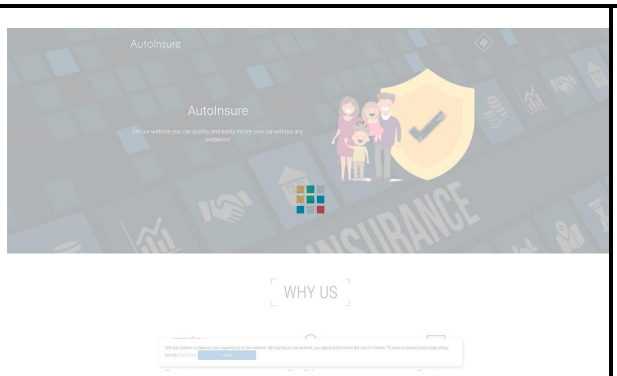
- Dridex IoCと同じ「pr-clanky」と「kvalitne」という文字列を含む638個のドメイン名

AutoITでコンパイルされたマルウェアのIoCを詳しく見る

AutoITでコンパイルされたマルウェアについて調査を広げるため、当社ではSANS ISCがIoCとして発表した3つのドメイン名、すなわちpublicpressmagazine[.]com、moscowkov[.]xyzおよびmoscowkov[.]atを使用しました。

まず、この3つのドメイン名をDNS lookupsで検索しました。その結果、172[.]67[.]137[.]212、104[.]21[.]81[.]36および85[.]209[.]135[.]159という3つのユニークなIPアドレスを発見しました。最初の2つは共用IPアドレスで、もう1つはプライベートなアドレスでした。また、2つは米国に、1つはオランダに所在していることがわかりました。

それらのIPアドレスをReverse IP/DNS lookupsで調べたところ、関連している可能性のあるドメイン名が329個見つかり、そのうち3%が悪意のドメイン名であることが判明しました。本稿執筆時点では、悪意あるドメイン名の大部分は到達不能でした。しかし、以下のページ（実際に使用されている自動車保険のサイト、売りに出ているサイトおよびインデックスページ）は、マルウェアのホストになったり、潜在的に危険なIPアドレスへ意図せずリンクしたりするかもしれず、レピュテーションリスクをはらんでいます。



bbbderwares[.]xyzのスクリーンショット

c5wult[.]cyouのスクリーンショット

heretopnewtopo[.]topのスクリーンショット

次に、IoCの中に見られる「publicpress」および「moscowkov」という文字列をキーワードとしてDomains & Subdomains Discoveryで検索した結果、関連している可能性のあるドメイン名154個がさらに見つかりました。今のところ悪意があると確認されたドメイン名はありませんが、AutoIT IoCと類似していることから、今後攻撃者にとって魅力的な脅威ベクトルとなる可能性があります。

新たなDridex攻撃を深掘り

最新のDridex攻撃については、IoCとして特定されたURL「http://pr-clanky[.]kvalitne[.]cz/65y3fd23d/87i4g3d2d2[.]exe」から調査を始めました。

まず、上記のURLから「pr-clanky[.]kvalitne[.]cz」を取り出し、その中の「kvalitne[.]cz」をhistorical WHOIS searchで検索しました。検索結果に無編集のメールアドレス「nfo@webzdarma[.]cz」が含まれていたため、それをもとに関連しそうなドメイン名が他にもないか探しました。結果として488個のドメイン名が見つかり、そのうちprodejce[.]czとweb2001[.]czは悪意あるドメイン名であることが確認されました。

DNS検索をしたところ、上記のドメイン名は185[.]64[.]219[.]6というIPアドレスに名前解決されることがわかりました。このIPアドレスは別の300個のドメイン名に共用されており、そのうちの1つ、11235813[.] webzdarma[.]cz は、悪意あるドメイン名でした。このドメイン名が、前述のhistorical WHOIS searchで見つかった無編集のメールアドレスのドメインと類似していることにご注意ください。このメールアドレスが2017年に使われていたことを考えると、旧来のDridex攻撃と最新のDridex攻撃の背後にいるアクターは同一の可能性があります。

さらに、IoCのドメイン名に含まれる「pr-clanky」と「kvalitne」という文字列をDomains & Subdomains Discoveryの検索キーワードとして使い、他の潜在的あるアーティファクトを収集しました。その結果、638個のドメイン名が発見されました。現時点でこれらのドメイン名は悪意があると特定されていません。しかし、IoCと似ていることから、最近発生したDridex攻撃の脅威アクターがこれらのドメイン名を将来マルウェアのホストとして使用するかもしれません。

脅威を早期に検知し、潜在的脅威ベクトルによるネットワークへのアクセスをブロックすることは、AutoITでコンパイルしたマルウェアやDridexのようなしつこいマルウェアを防ぐ有効な手段です。既存のIoCリストを広げることにより、マルウェアのエントリーポイントとなり得るものをすべて特定、監視することは、この手段に役立ちます。例えば、当社が今回行った徹底的な調査により、SANS ISCとTrend Microによる初期のIoCリストに12個の悪意あるドメイン名を含む1,425個のアーティファクトを追加することができました。

同様の調査をご希望のお客様、またはこの調査の全データをご希望のお客様は、こちらまでお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

SANS ISCが特定したAutoITのIoC

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

AutoIT IoCが名前解決したIPアドレスの例

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

AutoIT IoCと同じIPアドレスを使用していたドメイン名の例

- 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

AutoIT IoCと同じIPアドレスを使用していた悪意あるドメイン名の例

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

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

AutoIT IoCと同じ文字列を含むドメイン名の例

- 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

Trend Microが特定したDridex IoC

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

Dridex IoCと同じ連絡先メールアドレスを使用していたドメイン名の例

- 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

Dridex IoCと同じ連絡先メールアドレスを使用していた悪意あるドメイン名の例

- prodejce[.]cz

Dridex IoCが名前解決したIPアドレス

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

Dridex IoCと同じIPアドレスを使用していたドメイン名の例

- 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

Dridex IoCと同じIPアドレスを使用していた悪意あるドメイン名

- 11235813[.]webzdarma[.]cz

Dridex IoCと同じ文字列を含むドメイン名の例

- 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