What tracking an attacker email infrastructure tells us about persistent cybercriminal operations | Microsoft Security Blog

By Microsoft Threat Intelligence

Published: 2021-02-01 · Archived: 2026-04-05 15:51:16 UTC

From March to December 2020, we tracked segments of a dynamically generated email infrastructure that attackers used to send more than a million emails per month, distributing at least seven distinct malware families in dozens of campaigns using a variety of phishing lures and tactics. These campaigns aimed to deploy malware on target networks across the world, with notable concentration in the United States, Australia, and the United Kingdom. Attackers targeted the wholesale distribution, financial services, and healthcare industries.

By tracing these campaigns, we uncovered a sprawling infrastructure that is robust enough to seem legitimate to many mail providers, while flexible enough to allow the dynamic generation of new domain names and remain evasive. Shared IP space, domain generation algorithm (DGA) patterns, subdomains, registrations metadata, and signals from the headers of malicious emails enabled us to validate our research through overlaps in campaigns where attackers utilized multiple segments of purchased, owned, or compromised infrastructure. Using the intelligence we gathered on this infrastructure, we were at times able to predict how a domain was going to be used even before campaigns began.

This email infrastructure and the malware campaigns that use it exemplify the increasing sophistication of cybercriminal operations, driven by attackers who are motivated to use malware infections for more damaging, potentially more lucrative attacks. In fact, more recent campaigns that utilized this infrastructure distributed malware families linked to follow-on human-operated attacks, including campaigns that deployed Dopplepaymer, Makop, Clop, and other ransomware families.

Our deep investigation into this infrastructure brings to light these important insights about persistent cybercriminal operations:

- Tracking an email infrastructure surfaces patterns in attacker activity, bubbling up common elements in seemingly disparate campaigns
- Among domains that attackers use for sending emails, distributing malware, or command-and-control, the email domains are the most likely to share basic registration similarities and more likely to use DGA
- Malware services rely on proxy providers to make tracking and attribution difficult, but the proxies themselves can provide insights into upcoming campaigns and improve our ability to proactively protect against them
- Gaining intelligence on email infrastructures enables us to build or improve proactive and comprehensive protections like those provided by Microsoft Defender for Office 365 to defend against some of the world's most active malware campaigns

While there is existing in-depth research into some of these specific campaigns, in this blog we'll share more findings and details on how email distribution infrastructures drive some of the most prevalent malware operations today. Our goal is to provide important intelligence that hosting providers, registrars, ISPs, and email protection services can use and build on to protect customers from the threats of today and the future. We'll also share insights and context to empower security researchers and customers to take full advantage of solutions like Microsoft Defender for Office 365 to perform deep investigation and hunting in their environment and make their organizations resilient against attacks.

The role of for-sale infrastructure services in the threat ecosystem

We spotted the first segment of the infrastructure in March, when multiple domains were registered using distinct naming patterns, including the heavy use of the word "strange", inspiring the name StrangeU. In April, a second segment of the infrastructure, one that used domain generation algorithm (DGA), began registration as well. We call this segment RandomU.

The emergence of this infrastructure in March dovetailed with the disruption of the Necurs botnet that resulted in the reduction of service. Before being disrupted, Necurs was one of the world's largest botnets and was used by prolific malware campaign operators such as those behind Dridex. For-sale services like Necurs enable attackers to invest in malware production while leasing the delivery components of their activities to further obfuscate their behavior. The StrangeU and RandomU infrastructure appear to fill in the service gap that the Necurs disruption created, proving that attackers are highly motivated to quickly adapt to temporary interruptions to their operations.

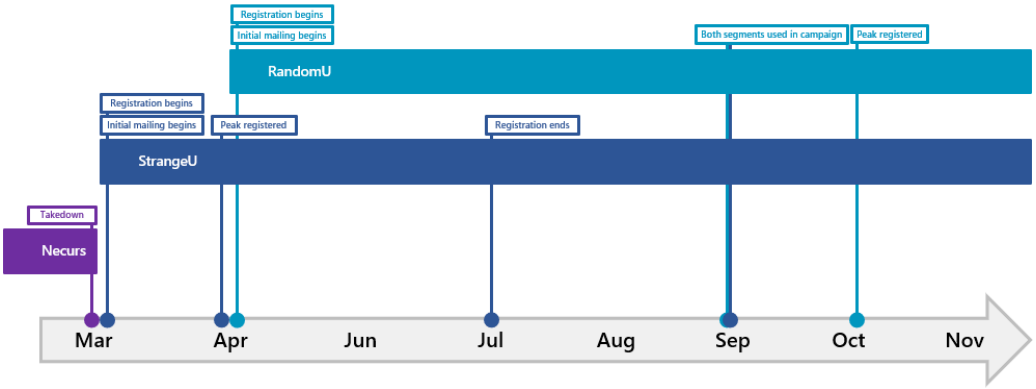

Figure 1. Timeline of staging and utilization of the email infrastructure

At first, the new email infrastructure was used infrequently in campaigns that distributed highly commodity malware like Mondfoxia and Makop. Soon, however, it attracted the attention of Dridex and Trickbot operators, who began using the infrastructure for portions of their campaigns, sometimes entirely and sometimes mixed with other compromised infrastructure or email providers.

Analyzing these mail clusters provides insight into how human the tangled web of modular attacker infrastructure remains. From unifying key traits in registration and behavior to the simple and effective techniques that the wide variety of malware uses, attackers' goals in this diversification point toward combatting automated analysis. However, these same shared characteristics and methods translate to insights that inform resilient protections that defend customers against these attacks.

Domain registration and email infrastructure staging

On March 7, 2020, attackers began registering a series of domains with Namecheap using sets of stolen email addresses, largely from free email services like mail.com, mail.ru, list.ru, and others. These domains all had similar characteristics that could be linked back to various similarities in registration. Almost all of the registered domains contained the word "strange" and were under the *.us* TLD, hence the name StrangeU. The use of *.us* TLD prevented domain or WHOIS privacy services—often used to obfuscate domain ownership and provenance—which are prohibited for this TLD.

To circumvent tracking and detection of these domains, attackers used false registration metadata. However, there was heavy crossover in the fake names and email addresses, allowing us to find additional domain names, some of which could be tied together using other keywords as shown in the list below, and fingerprint the domain generation mechanism.

The StrangeU domains were registered in early March 2020 and operated in continuous small bursts until April, when they were used for a large ransomware campaign. Following that, a new campaign occurred fairly regularly every few weeks. Registration of new domains continued throughout the year, and in September, the StrangeU infrastructure was used in conjunction with a similar infrastructure to deliver Dridex, after which these domains were used less frequently.

This second mailing segment, RandomU, employed a different DGA mechanism but still utilized Namecheap and showed a more consistent through line of registration metadata than its StrangeU counterpart. This infrastructure, which surfaced in April, was used infrequently through the Spring, with a surge in May and July. After the Dridex campaign in September in which it was used along with StrangeU, it has been used in two large Dridex campaigns every month.

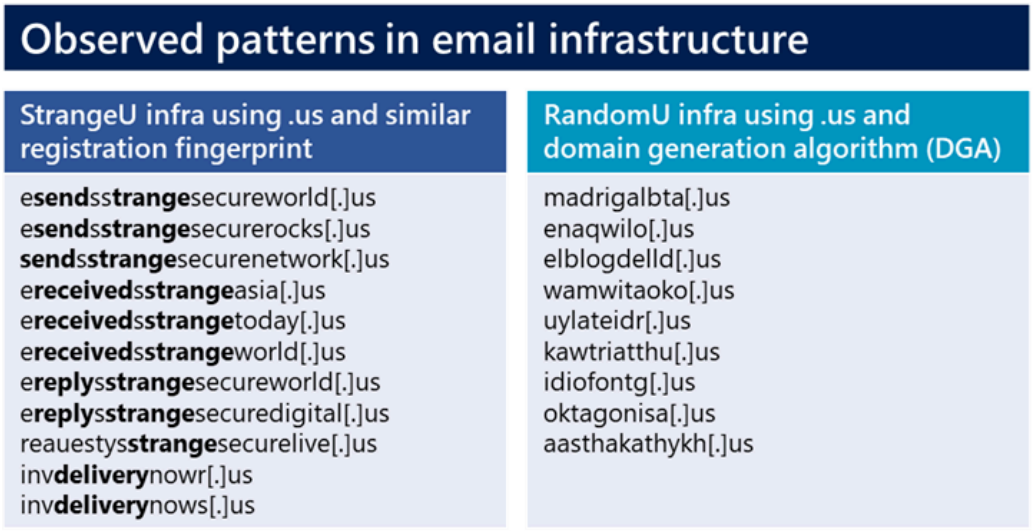

Figure 2. Common patterns in domains belonging to the email infrastructure

The StrangeU and RandomU segments of domains paint a picture of supplementing modular mailing services that allowed attackers to launch region-specific and enterprise-targeting attacks at scale, delivering over six million emails. The two segments contained a standard barrage of mailing subdomains, with over 60 unique subdomains referencing email across clusters, consistent with each other, with each domain having four to five subdomains. The following is a sample of malware campaigns, some of which we discuss in detail in succeeding sections, that we observed this infrastructure was used for:

- Korean spear-phishing campaigns that delivered Makop ransomware in April and June
- Emergency alert notifications that distributed Mondfoxia in April
- Black Lives Matter lure that delivered Trickbot in June
- Dridex campaign delivered through StrangeU and other infra from June to July
- Dofoil (SmokeLoader) campaign in August
- Emotet and Dridex activities in September, October, and November

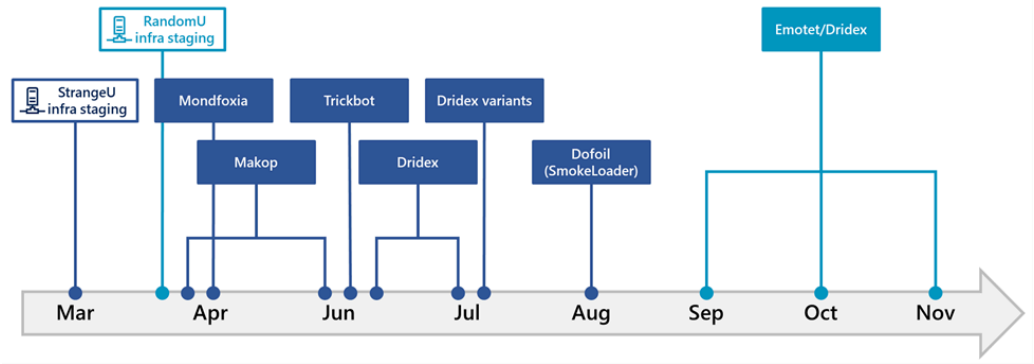

Figure 3. Timeline of campaigns that used StrangeU and RandomU domains

Korean spear-phishing delivers Makop ransomware (April and June 2020)

In early April, StrangeU was used to deliver the Makop ransomware. The emails were sent to organizations that had major business operations in Korea and used names of Korean companies as display names. Signals from Microsoft Defender for Office 365 indicated that these campaigns ran in short bursts.

The emails had *.zip* attachments containing executables with file names that resembled resumes from job seekers. Once a user opened the attachments, the executables delivered Makop, a ransomware-as-a-service (RaaS) payload that targeted devices and backups.

Upon infection, the malware quickly used the WMI command-line (WMIC) utility and deleted shadow copies. It then used the BCEdit tool and altered the boot configuration to ignore future failures and prevent restoration before encrypting all files and renaming them with *.makop* extensions.

The second time we observed the campaign almost two months later, in early June, the attackers used a Makop ransomware variant with many modified elements, including added persistence via scripts in the *Startup* folder before triggering a reboot.

Nearly identical attempts to deliver Makop using resume-based lures were covered by Korean security media during the entire year, using popular mail services through legitimate vendors like Naver and Hanmail. This could indicate that during short bursts the Makop operators were unable to launch their campaigns through legitimate services and had to move to alternate infrastructures like StrangeU instead.

Black Lives Matter lure delivers Trickbot (June 2020)

One campaign associated with the StrangeU infrastructure gained notoriety in mid-June for its lure as well as for delivering the notorious info-stealing malware Trickbot. This campaign circulated emails with malicious Word documents claiming to seek anonymous input on the Black Lives Matter movement.

An initial version of this campaign was observed on June 10 sending emails from a separate, unique attacker-owned mailing infrastructure using *.monster* domains. However, in the next iteration almost two weeks later, the campaign delivered emails from various domains specifically created with the Black Lives Matter signage, interspersed with StrangeU domains:

- b-lives-matter[.]site
- blivesm[.]space
- blivesmatter[.]site
- lives-matter-b[.]xyz
- whoslivesmatter[.]site
- lives-m-b[.]xyz
- ereceivedsstrangesecureworld[.]us
- b-l-m[.]site

Both campaigns carried the same Trickbot payload, operated for two days, and used identical post-execution commands and callouts to compromised WordPress sites.

Once a user opened the document attachment and enabled the malicious macro, Word launched *cmd.exe* with the command "*/c pause*" to evade security tools that monitored for successive launches of multiple processes. It then launched commands that deleted proxy settings in preparation for connecting to multiple C2 IP addresses.

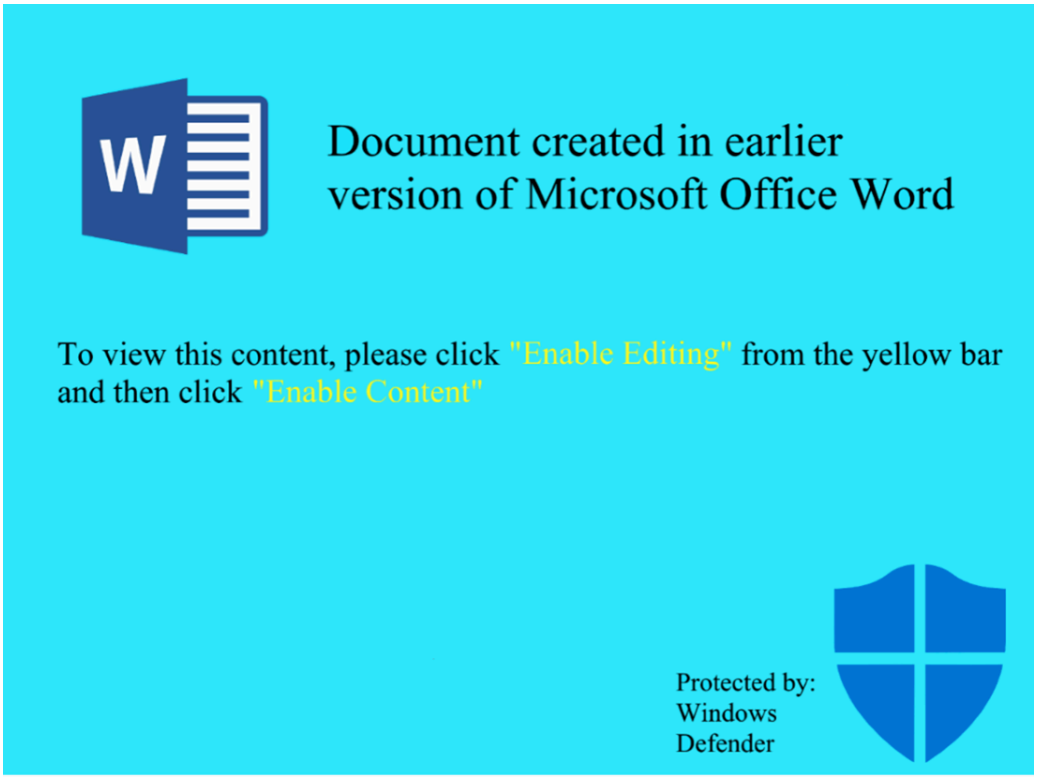

Figure 4. Screenshot of the malicious document used to deliver Trickbot

The commands also launched *rundll32.exe*, a native binary commonly used as a living-off-the-land binary, to load a malicious file in memory. The commandeered *rundll32.exe* also proceeded to perform other tasks using other living-off-the-land binaries, including *wermgr.exe* and *svchost.exe*.

In turn, the hijacked *wermgr.exe* process dropped a file with a *.dog* extension that appeared to be the Trickbot payload. The same instance of *wermgr.exe* then appeared to inject code into *svchost.exe* and scanned for open SMB ports on other devices. The commandeered *svchost.exe* used WMI to open connections to additional devices on the network, while continuing to collect data from the initial infected device. It also opened multiple browsers on localhost connections to capture browser history and other information via *esentutl.exe* and *grabber_temp.edb*, both of which are often used by the Trickbot malware family.

This campaign overwhelmingly targeted corporate accounts in the United States and Canada and avoided individual accounts. Despite heavy media coverage, this campaign was relatively small, reflecting a common behavior among cybercrime groups, which often run multiple, dynamic low-volume campaigns designed to evade resilient detection.

Dridex campaigns big and small (June to July 2020 and beyond)

From late June through July, Dridex operators ran numerous campaigns that distributed Excel documents with malicious macros to infect devices. These operators first delivered emails through the *StrangeU* infrastructure only, but they quickly started to use compromised email accounts of legitimate organizations as well, preventing defenders from easily blocking deliveries. Despite this, emails from either *StrangeU* or the compromised accounts had overlapping attributes. For example, many of the emails used the same *Reply To* addresses that were sourced from compromised individual accounts and not consistent with the sender addresses.

During the bulk of this run, Excel files were attached directly in the email in order to eventually pull the Dridex payload from .xyz domains such as those below. The attackers changed the delivery domains every few days and connected to IP-based C2s on familiar ports like 4664, 3889, 691, and 8443:

- yumicha[.]xyz

- rocesi[.]xyz
- secretpath[.]xyz
- guruofbullet[.]xyz
- Greyzone[.]xyz

When opened, the Excel document installed one of a series of custom Dridex executables downloaded from the attacker C2 sites. Like most variants in this malware family, the custom Dridex executables incorporated code loops, time delays, and environment detection mechanisms that evaded numerous public and enterprise sandboxes.

Dridex is known for its capability to perform credential theft and establish connectivity to attacker infrastructure. In this instance, the same Dridex payload was circulated daily using varying lures, often repeatedly to the same organizations to ensure execution on target networks.

During the longer and more stable Excel Dridex campaigns in June and July, a Dridex variant was also distributed in much smaller quantities utilizing Word documents over a one-day period, perhaps testing new evasion techniques. These Word documents, while still delivering Dridex, improved existing obfuscation methods using a unique combination of VBA stomping and replacing macros and function calls with arbitrary text. In a few samples of these documents, we found text from Shakespearean prose.

```
var farewell_and_moon = ["m","a","e","r","t","s",".","b","d","o","d","a"].reverse().join("")
```

```
a_painted_word(120888)
```

```
function as_thy_face(takes_from_hamlet)
```

```
{return new ActiveXObject(takes_from_hamlet)}
```

While Microsoft researchers didn't observe this portion of the campaign moving into the human-operated phase—targets did not open the attachment—this campaign was likely to introduce tools like PowerShell Empire or Cobalt Strike to steal credentials, move laterally, and deploy ransomware.

Emotet, Dridex, and the RandomU infrastructure (September and beyond)

Despite an errant handful of deliveries distributing Dofoil (also known as SmokeLoader) and other malware, the vast majority of the remaining deliveries through StrangeU have been Dridex campaigns that reoccured every few weeks for a handful of days at a time. These campaigns started on September 7, when RandomU and StrangeU were notably used in a single campaign, after which StrangeU began to see less utilization.

These Dridex campaigns utilized an Emotet loader and initial infrastructure for hosting, allowing the attackers to conduct a highly modular email campaign that delivered multiple distinct links to compromised domains. These domains employed heavy sandbox evasion and are connected by a series of PHP patterns ending in a small subset of options: *zxlbw.php*, *yymclv.php*, *zpsxxla.php*, or *app.php*. As the campaigns continued, the PHP was dynamically generated, adding other variants, including *vary.php*, *invoice.php*, *share.php*, and many others. Some examples are below.

- hxxps://molinolafama[.]com[.]mx/app[.]php
- hxxps://meetingmins[.]com/app[.]php
- hxxps://contrastmktg[.]com/yymclv[.]php
- hxxps://idklearningcentre[.]com[.]ng/zxlbw[.]php
- hxxps://idklearningcentre[.]com[.]ng/zpsxxla[.]php
- hxxps://idklearningcentre[.]com[.]ng/yymclv[.]php
- hxxps://hsa[.]ht/yymclv[.]php
- hxxps://hsa[.]ht/zpsxxla[.]php
- hxxps://hsa[.]ht/zxlbw[.]php
- hxxps://contrastmktg[.]com/yymclv[.]php
- hxxps://track[.]topad[.]co[.]uk/zpsxxla[.]php

- hxxps://seoemail[.]com[.]au/zxlbw[.]php
- hxxps://bred[.]fr-authentification-source-no[.]inaslimitada[.]com/zpsxxla[.]php
- hxxp://www[.]gbrecords[.]london/zpsxxla[.]php
- hxxp://autoblogsite[.]com/zpsxxla[.]php
- hxxps://thecrossfithandbook[.]com/zpsxxla[.]php
- hxxps://mail[.]168vitheyrealestate[.]com/zpsxxla[.]php

In this campaign, sandboxes were frequently redirected to unrelated sites like chemical manufacturers or medical suppliers, while users received an Emotet downloader within a Word document, which once again used macros to facilitate malicious activities.

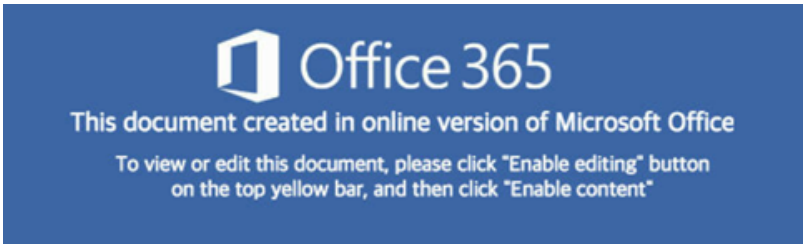

Figure 5. Screenshot of the malicious document used to deliver Dridex

The malicious macro utilized WMI to run a series of standard PowerShell commands. First, it downloaded the executable payload itself by contacting a series of C2 domains associated with Emotet campaigns since July. Afterward, additional encoded PowerShell commands were used in a similar fashion to download a .zip file that contained a Dridex DLL. Additional commands also reached out to a variety of Emotet infrastructure hosted on compromised WordPress administrative pages, even after the Dridex payload has already been downloaded. Dridex then modified RUN keys to automatically start the Dridex executable, which was renamed to riched20.exe on subsequent logons.

We also observed simultaneous connections to associated Dridex and Emotet infrastructure. These connections were largely unencrypted and occurred over a variety of ports and services, including ports 4664 and 9443. At this point the malware had firm presence on the machine, enabling attackers to perform human-operated activity at a later date.

In the past, reports have confirmed Dridex being delivered via leased Emotet infrastructure. There have also been many IP and payload-based associations. This research adds to that body of work and confirms additional associations via namespace, as well as correlation of email lure, metadata, and sender. This iteration of campaign repeated through October to December largely unchanged with nearly identical mails.

Defending organizations against malware campaigns

As attacks continue to grow in modularity, the tactics that attackers use to deliver phishing email, gain initial access on systems, and move laterally will continuously become more varied. This research shows that despite these disparities and the increased resiliency attackers have built, the core tactics and tools that they use are still limited in scope, relying repeatedly on familiar malicious macros, lures, and sending tactics.

Sweeping research into massive attacker infrastructures, as well as our real-time monitoring of malware campaigns and attacker activity, directly inform Microsoft security solutions, allowing us to build or improve protections that block malware campaigns and other email threats, both current and future, as well as provide enterprises with the tools for investigating and responding to email campaigns in real-time.

Microsoft delivers these capabilities through Microsoft Defender for Office 365. Features likes Safe attachments and Safe links ensure real-time, dynamic protection against email campaigns no matter the lure or evasion tactic. These features use a combination of detonation, automated analysis, and machine learning to detect new and unknown threats. Meanwhile, the Campaign view shows the complete picture of email campaigns as they happen, including timelines, sending patterns, impact to the organization, and details like IP addresses, senders, and URLs. These insights into email threats empower security operations teams to respond to attacks, perform additional hunting, and fix configuration issues.

Armed with an advanced solution like Microsoft Defender for Office 365 and the rest of technologies in the broader Microsoft 365 Defender solution, enterprises can further increase resilience against threats by following these recommendations:

- Educate end users about protecting personal and business information in social media, filtering unsolicited communication, identifying lures in spear-phishing email, and reporting of reconnaissance attempts and other suspicious activity.
- Configure Office 365 email filtering settings to ensure blocking of phishing & spoofed emails, spam, and emails with malware. Set Office 365 to recheck links on click and delete sent mail to benefit from newly acquired threat intelligence.
- Disallow macros or allow only macros from trusted locations. See the latest security baselines for Office and Office 365.
- Turn on AMSI for Office VBA.
- Check perimeter firewall and proxy to restrict servers from making arbitrary connections to the internet to browse or download files. Turn on network protection to block connections to malicious domains and IP addresses. Such restrictions help inhibit malware downloads and command-and-control activity.

Turning on attack surface reduction rules, including rules that can block advanced macro activity, executable content, process creation, and process injection initiated by Office applications, also significantly improves defenses. The following rules are especially useful in blocking the techniques observed in campaigns using the StrangeU and RandomU infrastructure:

- Block executable content from email client and webmail
- Block all Office applications from creating child processes
- Block Office applications from creating executable content
- Block Office applications from injecting code into other processes
- Block Win32 API calls from Office macros
- Block executable files from running unless they meet a prevalence, age, or trusted list criterion
- Block Javascript or VBScript from launching downloaded executable content
- Block execution of potentially obfuscated scripts

Microsoft 365 customers can also use the advanced hunting capabilities in Microsoft 365 Defender, which integrates signals from Microsoft Defender for Office 365 and other solutions, to locate activities and artifacts related to the infrastructure and campaigns discussed in this blog. These queries can be used with advanced hunting in Microsoft 365 security center, but the same regex pattern can be used on other security tools to identify or block emails.

This query searches for emails sent from *StrangeU e*mail addresses. Run query

```
EmailEvents
| where SenderMailFromDomain matches regex @"^(?:eraust|ereply|reply|ereceived|received|reaust|esend|inv|send|emailboost|eontaysstrange|eprop|frost|eont|servic(strange|stange|emailboost).*\.us$"
or SenderFromDomain matches regex @"^(?:eraust|ereply|reply|ereceived|received|reaust|esend|inv|send|emailboost|eontaysstrange|eprop|frost|eont|ser
```

Learn how you can stop attacks through automated, cross-domain security and built-in AI with Microsoft Defender 365.

Additional resources

- Listen to Episode 19 of the Security Unlocked podcast, where threat analyst Elif Kaya speaks about this email infrastructure
- Watch this Microsoft 365 Defender webinar about this research:

https://youtube.com/watch?v=scrs5Z0nsCk%3Ffeature%3Doembed

Indicators of compromise

StrangeU domains

esendsstrangeasia[.]us	sendsstrangesecuretoday[.]us	emailboostgedigital[.]us
emailboostgelife[.]us	emailboostgelifes[.]us	emailboostgesecureasia[.]us
eontaysstrangeasia[.]us	eontaysstrangenetwork[.]us	eontaysstrangerocks[.]us
eontaysstrangesecureasia[.]us	epropivedsstrangevip[.]us	ereplyggstangeasia[.]us
ereplyggstangedigital[.]us	ereplyggstangeereplys[.]us	ereplyggstangelifes[.]us
ereplyggstangenetwork[.]us	ereplyggstangesecureasia[.]us	frostsstrangeworld[.]us
servicceivedsstrangevip[.]us	servicplysstrangeasia[.]us	servicplysstrangedigital[.]us
servicplysstrangelife[.]us	servicplysstrangelifes[.]us	servicplysstrangenetwork[.]us
ereceivedsstrangesecureworld[.]us	ereceivedsstrangetoday[.]us	ereceivedsstrangeus[.]us
esendsstrangesecurelife[.]us	sendsstrangesecureesendss[.]us	ereplysstrangesecureasia[.]us
ereplysstrangesecurenetwork[.]us	receivedsstrangesecurelife[.]us	ereplysstrangeworld[.]us
reauestysstrangesecurelive[.]us	ereceivedsstrangeworld[.]us	esendsstrangesecurerocks[.]us
reauestysstrangesecuredigital[.]us	reauestysstrangesecurenetwork[.]us	reauestysstrangesecurevip[.]us
replysstrangesecurelife[.]us	ereauestysstrangesecurerocks[.]us	ereceivedsstrangeasia[.]us
ereceivedsstrangedigital[.]us	ereceivedsstrangeereceiveds[.]us	ereceivedsstrangelife[.]us
ereceivedsstrangelifes[.]us	ereceivedsstrangenetwork[.]us	ereceivedsstrangerocks[.]us
ereceivedsstrangesecureasia[.]us	receivedsstrangeworld[.]us	replysstrangedigital[.]us
invdeliverynows[.]us	esendsstrangesecuredigital[.]us	esendsstrangesecureworld[.]us
sendsstrangesecurenetwork[.]us	ereceivedsstrangevip[.]us	replysstrangerocs[.]us
replysstrangesecurelive[.]us	invpaymentnoweros[.]us	invpaymentnowes[.]us
replysstrangeracs[.]us	reauestysstrangesecurebest[.]us	receivedsstrangesecurebest[.]us
reauestysstrangesecurelife[.]us	ereplysstrangevip[.]us	reauestysstrangesecuretoday[.]us
ereplysstrangesecureus[.]us	ereplysstrangetoday[.]us	ereceivedsstrangesecuredigital[.]us
ereceivedsstrangesecureereceiveds[.]us	ereceivedsstrangesecurelife[.]us	ereceivedsstrangesecurenetwork[.]us
ereceivedsstrangesecurerocks[.]us	ereceivedsstrangesecureus[.]us	ereceivedsstrangesecurevip[.]us
sendsstrangesecurebest[.]us	sendsstrangesecuredigital[.]us	sendsstrangesecurelive[.]us
sendsstrangesecureworld[.]us	esendsstrangedigital[.]us	esendsstrangeesends[.]us
esendsstrangelifes[.]us	esendsstrangerocks[.]us	esendsstrangesecureasia[.]us
esendsstrangesecureesends[.]us	esendsstrangesecurenetwork[.]us	esendsstrangesecureus[.]us

esendsstrangesecurevip[.]us	esendsstrangevip[.]us	ereauestysstrangesecureasia[.]us
ereplysstrangeasia[.]us	ereplysstrangedigital[.]us	ereplysstrangeereplys[.]us
ereplysstrangelife[.]us	ereplysstrangelifes[.]us	ereplysstrangenetwork[.]us
ereplysstrangerocks[.]us	ereplysstrangesecuredigital[.]us	ereplysstrangesecureereplys[.]us
ereplysstrangesecurelife[.]us	ereplysstrangesecurerocks[.]us	ereplysstrangesecurevip[.]us
ereplysstrangesecureworld[.]us	ereplysstrangeus[.]us	reauestysstrangesecureclub[.]us
reauestysstrangesecureereauestyss[.]us	reauestysstrangesecureworld[.]us	receivedsstrangesecureclub[.]us
receivedsstrangesecuredigital[.]us	receivedsstrangesecureereceivedss[.]us	receivedsstrangesecurelive[.]us
receivedsstrangesecurenetwork[.]us	receivedsstrangesecuretoday[.]us	receivedsstrangesecurevip[.]us
receivedsstrangesecureworld[.]us	replysstrangesecurebest[.]us	replysstrangesecureclub[.]us
replysstrangesecuredigital[.]us	replysstrangesecureereplyss[.]us	replysstrangesecurenetwork[.]us
replysstrangesecuretoday[.]us	replysstrangesecurevip[.]us	replysstrangesecureworld[.]us
sendsstrangesecurevip[.]us	esendsstrangelife[.]us	esendsstrangenetwork[.]us
esendsstrangetoday[.]us	esendsstrangeus[.]us	esendsstrangeworld[.]us
sendsstrangesecureclub[.]us	sendsstrangesecurelife[.]us	plysstrangelifes[.]us
intulifeinoi[.]us	replysstrangerocks[.]us	invpaymentnowe[.]us
replysstrangelifes[.]us	replysstrangenetwork[.]us	invdeliverynowr[.]us
ereceivedggstangevip[.]us	ereplyggstangerocks[.]us	servicceivedsstrangeworld[.]us
servicplysstrangesecureasia[.]us	servicplysstrangeservicplys[.]us	emailboostgeasia[.]us
emailboostgeereplys[.]us	emailboostgenetwork[.]us	emailboostgerocks[.]us
eontaysstrangedigital[.]us	eontaysstrangeeontays[.]us	eontaysstrangelife[.]us
eontaysstrangelifes[.]us	epropivedsstrangeworld[.]us	ereceivedggstangeworld[.]us
ereplyggstangelife[.]us	frostsstrangevip[.]us	servicplysstrangerocks[.]us
invdeliverynow[.]us	invpaymentnowlife[.]us	invdeliverynowes[.]us
invpaymentnowwork[.]us	replysstrangedigitals[.]us	replysstrangelife[.]us
replysstrangelifee[.]us	replystrangeracs[.]us	

RandomU domains

cnewyllansf[.]us	kibintiwl[.]us	planetezs[.]us	sakgeldvi[.]us
rdoowvaki[.]us	kabelrandjc[.]us	wembaafag[.]us	postigleip[.]us
jujubugh[.]us	honidefic[.]us	utietang[.]us	scardullowv[.]us
vorlassebv[.]us	jatexono[.]us	vlevaiph[.]us	bridgetissimema[.]us

schildernjc[.]us	francadagf[.]us	strgatibp[.]us	jelenskomna[.]us
prependerac[.]us	oktagonisa[.]us	enjaularszr[.]us	opteahzf[.]us
skaplyndiej[.]us	dirnaichly[.]us	kiesmanvs[.]us	gooitounl[.]us
izvoznojai[.]us	kuphindanv[.]us	pluienscz[.]us	huyumajr[.]us
arrutisdo[.]us	loftinumkx[.]us	ffermwyrzf[.]us	hectorfranez[.]us
munzoneia[.]us	savichicknc[.]us	nadurogak[.]us	raceaddicteg[.]us
mpixiris[.]us	lestenas[.]us	collahahhaged[.]us	enayilebl[.]us
hotteswc[.]us	kupakiliayw[.]us	deroutarek[.]us	pomagatia[.]us
mizbebzpe[.]us	firebrandig[.]us	univerzamjw[.]us	amigosenrutavt[.]us
kafrdaaia[.]us	cimadalfj[.]us	ubrzanihaa[.]us	yamashumiks[.]us
jakartayd[.]us	cobiauql[.]us	idiofontg[.]us	hoargettattzt[.]us
encilips[.]us	dafanapydutsb[.]us	intereqr[.]us	chestecotry[.]us
diegdoceqy[.]us	ffwdenaiszh[.]us	sterinaba[.]us	wamwitaoko[.]us
peishenthe[.]us	hegenheimlr[.]us	educarepn[.]us	ayajuaqo[.]us
imkingdanuj[.]us	dypeplayentqt[.]us	traktorkaqk[.]us	prilipexr[.]us
collazzird[.]us	sentaosez[.]us	vangnetxh[.]us	valdreska[.]us
mxcujatr[.]us	angelqtbw[.]us	bescromeobsemyb[.]us	hoogametas[.]us
mlitavitiwj[.]us	pasgemaakhc[.]us	facelijaxg[.]us	harukihotarugf[.]us
pasosaga[.]us	mashimariokt[.]us	vodoclundqs[.]us	trofealnytw[.]us
cowboyie[.]us	dragovanmm[.]us	jonuzpura[.]us	cahurisms[.]us
leetzetli[.]us	jonrucunopz[.]us	flaaksik[.]us	wizjadne[.]us
zatsopanogn[.]us	roblanzq[.]us	barbwirelx[.]us	givolettoan[.]us
gyfarosmt[.]us	zastirkjx[.]us	sappianoyv[.]us	noneedfordayvnb[.]us
andreguidiao[.]us	concubinsel[.]us	meljitebj[.]us	alcalizezsc[.]us
springenmw[.]us	kongovkamev[.]us	starlitent[.]us	cassineraqy[.]us
ariankacf[.]us	plachezxr[.]us	abulpasastq[.]us	scraithehk[.]us
wintertimero[.]us	abbylukis[.]us	lumcrizal[.]us	trokrilenyr[.]us
skybdragonqx[.]us	pojahuez[.]us	rambalegiec[.]us	relucrarebk[.]us
vupardoumeip[.]us	punicdxak[.]us	vaninabaranaogw[.]us	yesitsmeagainle[.]us
upcominge[.]us	arwresaub[.]us	zensimup[.]us	joelstonem[.]us
ciflaratzz[.]us	adespartc[.]us	maaltijdr[.]us	acmindiaj[.]us
mempetebyj[.]us	itorandat[.]us	galenicire[.]us	cheldisalk[.]us

zooramawpreahkt[.]us	sijamskojoc[.]us	fliefedomrr[.]us	ascenitianyrg[.]us
tebejavaaq[.]us	finnerssshu[.]us	slimshortyub[.]us	angstigft[.]us
avedaviya[.]us	aasthakathykh[.]us	nesklonixt[.]us	drywelyza[.]us
paginomxd[.]us	gathesitehalazw[.]us	antinodele[.]us	ferestat[.]us
tianaoeuat[.]us	pogilasyg[.]us	mjawxxik[.]us	bertolinnj[.]us
auswalzenna[.]us	mmmikeyvb[.]us	megafonasgc[.]us	litnanjv[.]us
boockmasi[.]us	andreillazf[.]us	vampirupn[.]us	lionarivv[.]us
ihmbklkdk[.]us	okergeeliw[.]us	forthabezb[.]us	trocetasss[.]us
kavamennci[.]us	mipancepezc[.]us	infuuslx[.]us	dvodomnogeg[.]us
zensingergy[.]us	eixirienhj[.]us	trapunted[.]us	greatfutbolot[.]us
porajskigx[.]us	mumbleiwa[.]us	cilindrarqe[.]us	uylateidr[.]us
sdsandrahuin[.]us	trapeesr[.]us	trauttbobw[.]us	bostiwro[.]us
niqiniswen[.]us	ditionith[.]us	folseine[.]us	zamoreki[.]us
sonornogae[.]us	xlsadlxg[.]us	varerizu[.]us	seekabelv[.]us
nisabooz[.]us	pohvalamt[.]us	inassyndr[.]us	ivenyand[.]us
karbonsavz[.]us	svunturc[.]us	babyrosep[.]us	aardigerf[.]us
fedrelandx[.]us	degaeriah[.]us	detidiel[.]us	acuendoj[.]us
peludine[.]us	impermatav[.]us	datsailis[.]us	melenceid[.]us
beshinon[.]us	dinangnc[.]us	fowiniler[.]us	laibstadtws[.]us
bischerohc[.]us	muctimpubwz[.]us	jusidalikan[.]us	peerbalkw[.]us
robesikaton[.]us	thabywnderlc[.]us	osoremep[.]us	krlperuoe[.]us
ntarodide[.]us	bideoskin[.]us	senagena[.]us	kelyldori[.]us
kawtriatthu[.]us	rbreriaf[.]us	enaqwilo[.]us	monesine[.]us
onwinaka[.]us	yonhydro[.]us	siostailpg[.]us	bannasba[.]us
milosnicacz[.]us	tunenida[.]us	sargasseu[.]us	malayabc[.]us
prokszacd[.]us	premarketcl[.]us	zedyahai[.]us	xinarmol[.]us
minttaid[.]us	pufuletzpb[.]us	nekbrekerdv[.]us	ppugsasiw[.]us
katarkamgm[.]us	kyraidaci[.]us	falhiblaqv[.]us	lisusant[.]us
mameriar[.]us	quslinie[.]us	nirdorver[.]us	trocairasec[.]us
pochwikbz[.]us	ingykhat[.]us	okrzynjf[.]us	razsutegayl[.]us
dimbachzx[.]us	buchingmc[.]us	iessemda[.]us	fatarelliqi[.]us
efetivumd[.]us	vdevicioik[.]us	klumppwha[.]us	stefiensi[.]us

donetzbx[.]us	wetafteto[.]us	denementnd[.]us	cyllvysr[.]us
viweewmokmt[.]us	destescutyi[.]us	craulisrt[.]us	maggiebagglesxt[.]us
yawapasaqi[.]us	spimilatads[.]us	paseadoryy[.]us	apageyantak[.]us
magicofaloeaj[.]us	prefatoryhe[.]us	statvaiq[.]us	piketuojaqk[.]us
mushipotatobt[.]us	suergonugoy[.]us	gummiskoxt[.]us	torunikc[.]us
adoleishswn[.]us	rovljanie[.]us	ivicukfa[.]us	vajarelliwe[.]us
burksuit[.]us	adoraableio[.]us	bassettsz[.]us	chevyguyxq[.]us
lunamaosa[.]us	telemovelmi[.]us	pimptazticui[.]us	posteryeiq[.]us
miriamloiso[.]us	salahlekajl[.]us	inveshilifj[.]us	alquicelbi[.]us
hitagjafirt[.]us	ohatranqm[.]us	scosebexgofxu[.]us	vivalasuzyygb[.]us
lugleeghp[.]us	alicuppippn[.]us	wedutuanceseefv[.]us	abnodobemmn[.]us
zajdilxtes[.]us	inhaltsqxw[.]us	rejtacdat[.]us	contunaag[.]us
pitajucmas[.]us	delopezmc[.]us	donjimafx[.]us	iheartcoxlc[.]us
rommelcrxgi[.]us	jorguetky[.]us	jadesellvb[.]us	fintercentrosfs[.]us
ralbarix[.]us	kynnirinnty[.]us	bibulbio[.]us	aspazjagh[.]us
gleboqrat[.]us	tensinory[.]us	usitniterx[.]us	zaretkyui[.]us
hentugustqy[.]us	surigatoszuk[.]us	nitoeranybr[.]us	spitzkopuo[.]us
podkarpatruszz[.]us	milfincasqo[.]us	datatsbjew[.]us	changotme[.]us
losbindebt[.]us	ninjachuckvb[.]us	desfadavacp[.]us	potkazatiun[.]us
sernakct[.]us	razmersat[.]us	purtinaah[.]us	ampiovfa[.]us
durstinyskv[.]us	kreukenct[.]us	shinanyavc[.]us	kolaryta[.]us
yangtsekk[.]us	voyagedeviema[.]us	elblogdelld[.]us	utiligijc[.]us
peaplesokqo[.]us	jenggoteq[.]us	dogliairler[.]us	kandizifb[.]us
flunkmasteraz[.]us	clewpossejj[.]us	hymgaledaja[.]us	gmckayar[.]us
fagordul[.]us	pnendickhs[.]us	arrogede[.]us	stilenii[.]us
cafelireao[.]us	poishiuuz[.]us	nonfunccoupyo[.]us	madrigalbta[.]us
tarad[.]us	sarahcp[.]us	wickyjr[.]us	ghadrn[.]us
sirvond[.]us	qumarta[.]us	verow[.]us	mondeki[.]us
lirana[.]us	niarvi[.]us	belena[.]us	qucono[.]us
ulianag[.]us	lenut[.]us	shivave[.]us	jendone[.]us
seddauf[.]us	jarare[.]us	uchar[.]us	ealesa[.]us
wyoso[.]us	marnde[.]us	thiath[.]us	aulax[.]us

bobelil[.]us	jestem[.]us	detala[.]us	phieyen[.]us
annazo[.]us	dilen[.]us	jelan[.]us	ipedana[.]us
keulsph[.]us	ztereqm[.]us	rinitan[.]us	natab[.]us
haritol[.]us	ricould[.]us	lldra[.]us	miniacs[.]us
zahrajr[.]us	cayav[.]us	pheduk[.]us	qugagad[.]us
dehist[.]us	letama[.]us	mencyat[.]us	vindae[.]us
uranc[.]us	handil[.]us	galezay[.]us	bamerna[.]us
yllyn[.]us	ckavl[.]us	ilalie[.]us	daellee[.]us
cuparoc[.]us	zelone[.]us	burnile[.]us	uloryrt[.]us
shexo[.]us	phalbe[.]us	hanolen[.]us	lorria[.]us
beten[.]us	xuserye[.]us	iclelan[.]us	cwokas[.]us
vesic[.]us	ontolan[.]us	wajdana[.]us	telama[.]us
missani[.]us	usinaye[.]us	ertanom[.]us	kericex[.]us
denaga[.]us	tyderq[.]us	seliza[.]us	kinnco[.]us
qurtey[.]us	arzenitlu[.]us	vellpoildzu[.]us	keityod[.]us
ltangerineldf[.]us	lizergidft[.]us	serrucheah[.]us	lolricelolad[.]us
expiantaszg[.]us	hljqfyky[.]us	abarrosch[.]us	lepestrinynr[.]us
elektroduendevq[.]us	waggonbauwh[.]us	chaquetzgg[.]us	revizijiqa[.]us
ziggyiqta[.]us	rokenounkaf[.]us	lottemanvl[.]us	corsetatsvp[.]us
extasiatny[.]us	darkinjtat[.]us	pastorsta[.]us	sategnaxf[.]us
mordiquedp[.]us	mogulanbub[.]us	aleesexx[.]us	strekktumgz[.]us
kresanike[.]us	oberhirtesn[.]us	wyddiongw[.]us	etherviltjd[.]us
gdinauq[.]us	tumisolcv[.]us	oardbzta[.]us	zamislimrx[.]us
tidifkil[.]us	anwirbtda[.]us	breliaattainoqt[.]us	steinzeitps[.]us
grafoay[.]us	shuramiok[.]us	sanarteau[.]us	jerininomgv[.]us
kusturirp[.]us	tenisaragonpu[.]us	terquezajf[.]us	remularegf[.]us
nobanior[.]us	julijmc[.]us	dekrapp[.]us	odaljenakd[.]us

Source: https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/