DECEPTION AT SCALE: HOW ATTACKERS ABUSE GOVERNMENTAL INFRASTRUCTURE

VIRUSTOTAL

Nov 22

Welcome

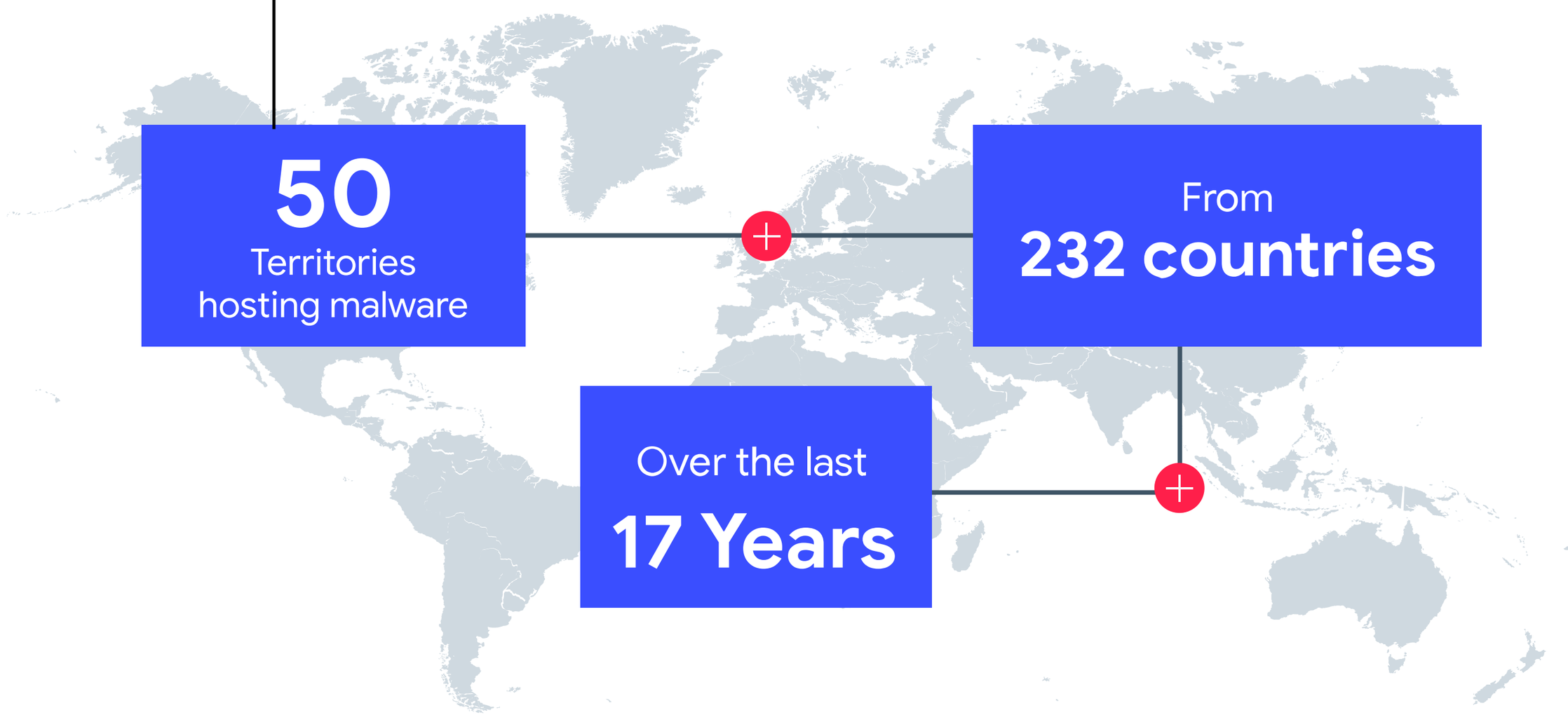
Welcome to the VirusTotal **“Deception at scale: How attackers abuse governmental infrastructure”** research report. We hope that by sharing our visibility into the threat landscape, we can help researchers, security practitioners, and the public better understand the evolution of malware attacks. This report explores how attackers abuse governmental-related infrastructure for their attacks.

There are thousands of domains that are directly or indirectly related to governmental organizations. Government domains are often trusted implicitly and therefore usually considered safe, but one of the consequences of presuming security is that expectation reduces the chances of detecting or blocking an attack. That’s exactly why malicious hackers find them appealing targets: They can be used as stepping stones to reach bigger targets, and they can be used to target victims for massive malware distribution.

During our research, we found dozens of government sites in more than 50 territories hosting malware – including trojans, phishing, banking malware, ransomware, and lateral movement tools. In some cases, we found indications that hacked government-affiliated sites had been used in targeted attacks. We also found traces of compromised sites and proof of dozens of sites distributing webshells. In many cases, we believe sites were poorly maintained and their compromised infrastructure was sometimes the result of collateral damage from other widespread infections.

VirusTotal is in a unique position to provide a source of comprehensive visibility of the malware landscape. Over the last 17 years, we have processed more than two million files per day across 232 countries. VirusTotal also harnesses contributions of its community of users to provide relevant attack context. We use this crowdsourced intelligence to analyze relevant data, share an understanding of how attacks develop, and help inform how they might evolve in the future.

This report contributes to what we hope will become an ongoing community effort to discover and share actionable information on malware trends.



Executive Summary

⚠ **Governmental domains** are among the **top categories** used by attackers in 2022 to distribute malicious content.

⚠ We found **dozens of government-related domains hosting many kinds of malware**, including trojans, ransomware, phishing, coin miners, banking malware, and lateral movement tools.

⚠ Although some affected domains seem to be **victims of opportunistic attacks**, there are indicators that some of them were targeted by sophisticated attackers who abused their infrastructure to deploy their toolsets.

⚠ Using **legitimate government domains for malware hosting** can enable an attacker to improve the efficiency of social engineering attacks and avoid defenses and alerts based on deny/allow lists.

⚠ We also found **traces of various webshells** hosted in dozens of governmental domains.

⚠ More generally, we observed an **increase of phishing levels in 2022** along with a large distribution of suspicious PDFs. Recently created XLSX files seem to replace DOCX as the preferred mechanism to distribute malware.

Methodology

VirusTotal relies on crowdsourced contributions, which provide a valuable picture of how different attacks spread and evolve. All data in this report is compiled using a representative subset of submissions from our users.

The relevance of the samples observed and detected as malicious varies throughout the year. Small changes in malicious samples driven by variances in contributors, polymorphism, and external crawlers can result in significantly more unique detections.

Abuse of governmental-related infrastructure

Following our previous Deception at Scale report, which focused on how malware abuses trust, we explored how some particularly sensitive domains were abused by attackers in more detail. In particular, we looked at government-related domains and the type of malicious activity in which they were involved. This report offers detailed examples as well as summary analyses of such attacks.

What type of domains are most abused by attackers?

We used antivirus domain categorization, as provided by several vendors in VirusTotal and additional content filtering solutions, to identify the categories (based on the economic sector they belong) most prone to abuse. Although antivirus vendor verdicts for domains are simpler than those they provide for samples, the information they provide is valuable. The following chart shows the evolution of detections on suspicious domains between 2022 and previous years, where we observe an increase in the percentage of domains categorized as phishing.

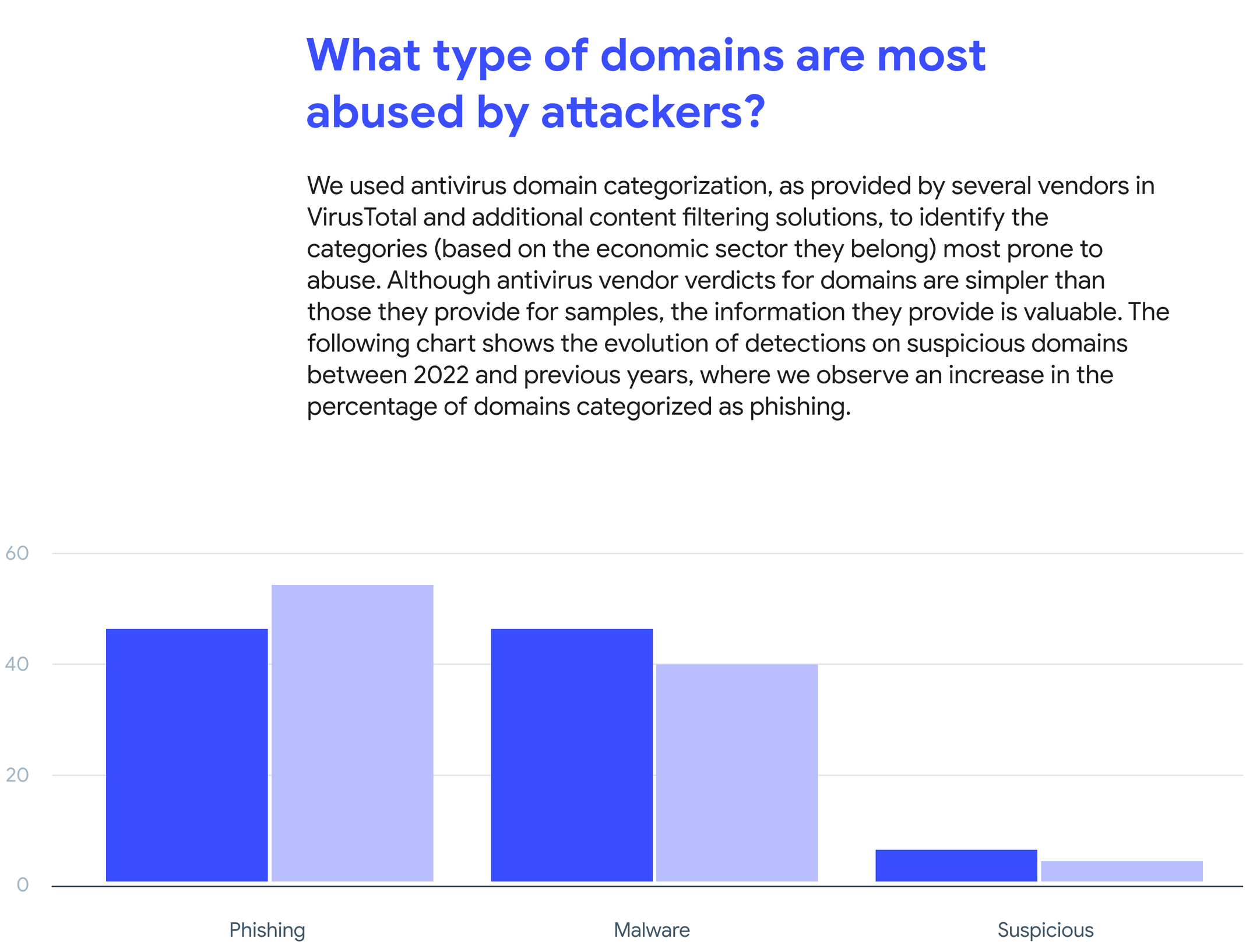


Fig 1.

Phishing vs Malware domain distribution timeline (%)

Antivirus vendor domain categories also provide insights on the nature of the suspicious domain. After normalizing and cleaning the data, the following chart shows top suspicious domains' categories for 2022:

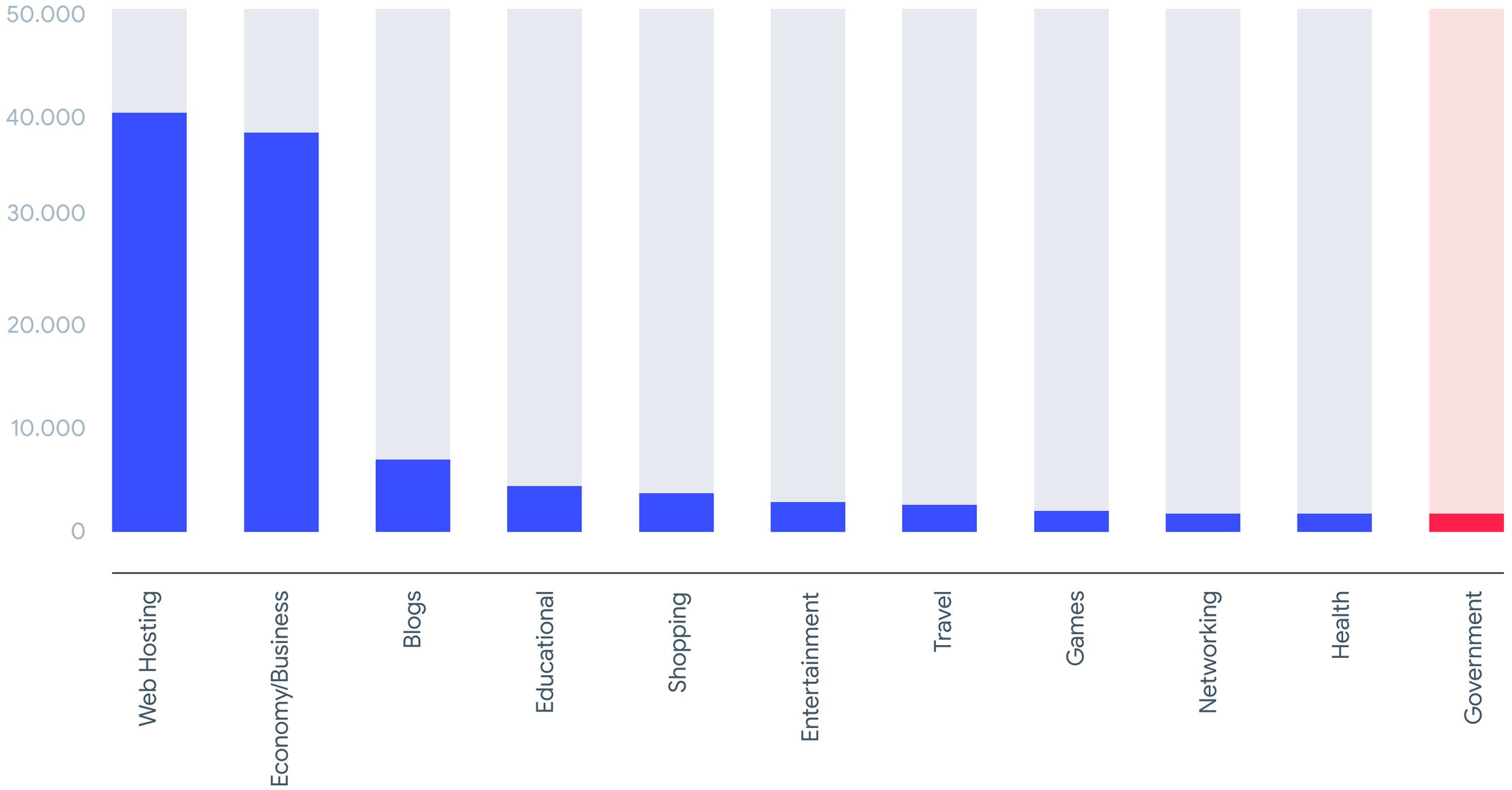


Fig 2.

Top domain categories abused by attackers in 2022

The chart is limited by the categories provided by antivirus software. Web hosting, by its nature, was expected to be largely abused, followed at a different scale by blogs. Unfortunately the Economy/Business category appears to be far too broad in its segmentation criteria to offer any chance of meaningful analysis. Educational institutions are usual targets for both targeted and opportunistic attacks, but are at a similar level when compared to the rest of the categories. We want to underline that the Government category also appears as one of the top abused ones over other categories such as forums, real estate or lifestyle.

Domains can be labeled as suspicious for a number of reasons, including spreading malware. The following chart provides a breakdown of types of suspicious files found distributed in the wild by the previous suspicious domains:

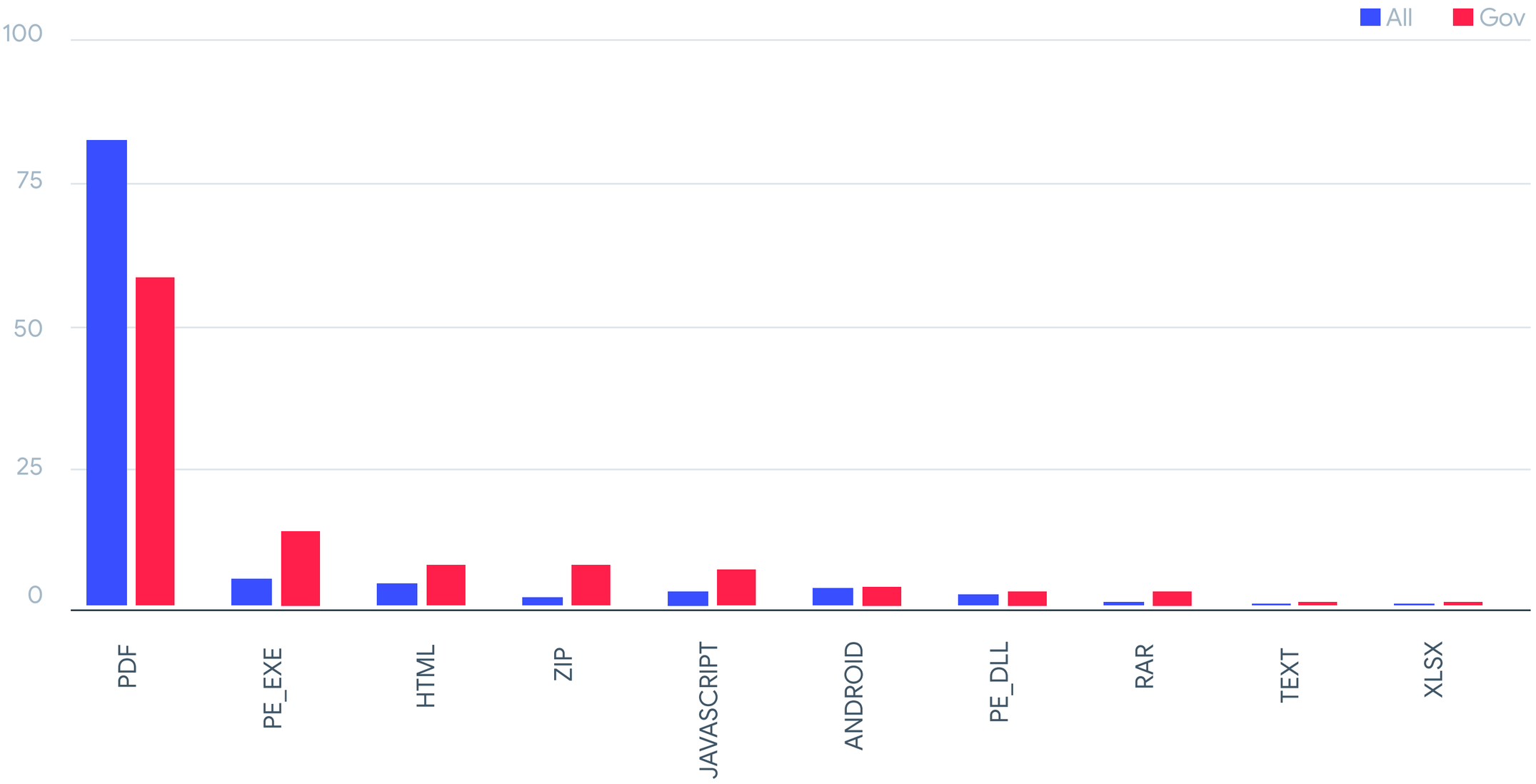


Fig 3.

Top suspicious samples' type distributed in the wild in 2022 (%)

PDF is the most commonly-distributed file type sent from suspicious domains and used for malware distribution and phishing. Windows executable files are the second most common file type, followed by HTML which often corresponds to malicious sites trying to infect visitors, similar to Javascript in fifth place.

Android shows a different picture as most of the samples found were distributed through rogue marketplaces (most of them from China) and, in 85% of cases, are detected by antivirus as Potential Unwanted Applications or Adware. We want to note the presence of XLSX format in this list along with the absence of DOCX, which is a trend we already observed in our previous Malware Trends report.

When comparing the generic trend of suspicious file distribution versus government domains, there is a huge difference in the percentage of PDF files (81% generic domains vs 57% governmental domains). This naturally results in an increase for all other file types distributed from governmental-related domains. This is especially notable for Windows executable, Javascript and XLSX files (3 times more) and for ZIP (4.5 times more).

Other than the file types, it is also important to know how “fresh” the distributed samples are. The following chart shows the percentage of samples per type we observed for the first time in VirusTotal in 2022:

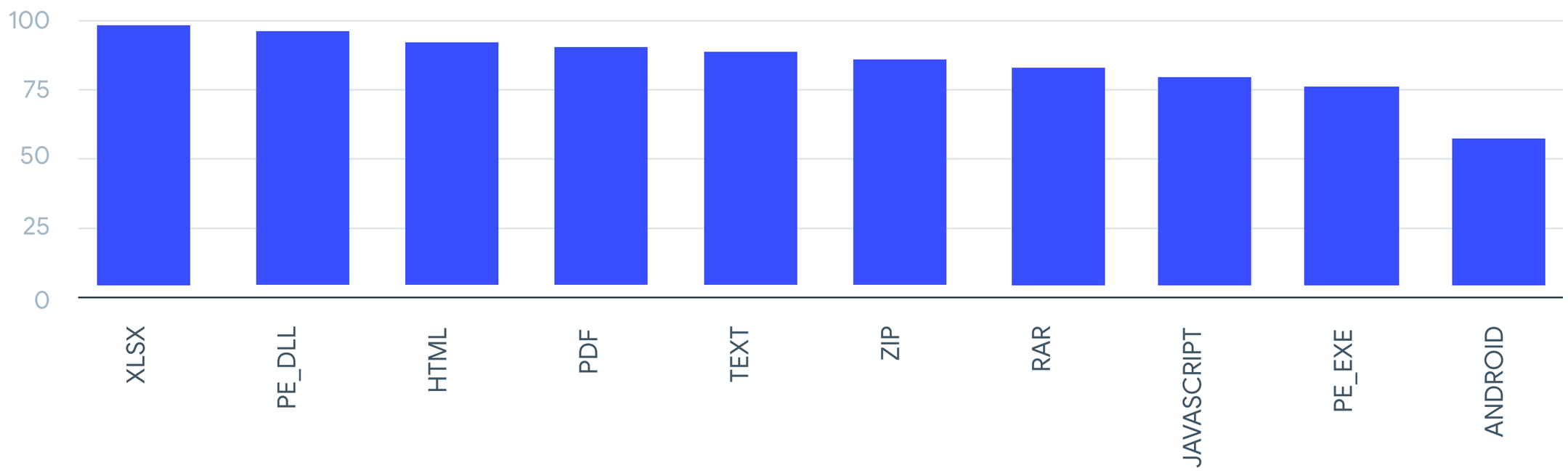


Fig 4.

Malware distributed in the wild in 2022 'freshness' by file type (%)

XLSX is the top one in this chart, doubling down on the distribution trend previously discussed. HTML was expected to be the “fresher” format by its nature, but surprisingly DLLs take this position even above PEs (by 20 percentage points). Android samples, also by its distribution nature mostly through marketplaces, seem not to be so frequently updated. For all types distributed in the wild, except Android, VirusTotal saw over 75% of them for the first time during 2022.

As a quick summary, we observed Government websites in the top categories for malicious content distribution. During the year, we observed a general growth in phishing distribution. PDF is the most popular format found to distribute malicious content in the wild. XLSX is quickly replacing other office formats for malware distribution. When attackers get the chance to compromise Government infrastructure, they aggressively use the opportunity to distribute malware executables.

Government-related domains

Domains belonging to any government-related institution, by obvious reasons, are a sought after target for attackers. This doesn’t necessarily mean these domains are the final target of the attack, or that the attackers belong to any APT group. Although this could also be the case, we found examples where victims seem to be the target of opportunistic cybercriminal attacks, or where attackers simply used them as stepping stones for an ongoing campaign.

In this section, we collected several interesting representative examples we found when analyzing in detail different government-related suspicious activity.

The following chart shows top TLDs for government-related suspicious domains we found in VirusTotal in 2022. We decided to exclude non-specific TLDs (such as .com, .net, .org, etc) from this list:

Fig 5.

Top government TLDs distributing suspicious samples in 2022, by country

The previous list is based on suspicious domains according to antivirus, so there is a relatively high chance of false positives. For the rest of this section, we manually double-checked different interesting representative cases on how attackers abused government-related domains in different scenarios.

Opportunistic attacks

We define ´opportunistic´ as attacks where the target was randomly chosen.

A governmental initiative in Guatemala hosted a number of malicious samples, including a PDF invoice used as part of a social engineering attack. This PDF was heavily used in different attacks between July and August 2022, including ransomware. We speculate attackers simply found an easy target to host their malware, likely using automatic methods.

Trojans and droppers

These attacks serve first stagers that can be used for different purposes.

A Chinese municipality site hosted a malicious sample under a couple of subdomains, first seen in VirusTotal in 2017 and hosted in the legitimate domain for almost three years under different URLs. The sample is a Windows trojan with keylogger and screenshot capabilities, disguised as a popular compression Chinese utility under the “Download” path of the website.

We found malware with similar capabilities coming from a government office website in Bangladesh. However, telemetry indicates it was hosted for around three months.

A Peruvian governmental site hosted a sample of the dangerous njRAT. This particular sample was first seen in November 2021, and the site already cleaned it up at the time of writing this report.

We cannot speculate the purpose of these cases, as they can be either used for mass distribution or for specific targeted attacks. However, the impact can be severe depending on the traffic of these trusted websites.

Bankers

We observed several banking phishing attacks abusing governmental infrastructure – and in some cases, we also detected hosted banking trojans, still popular in some countries.

We found an Indonesian governmental entity hosting several Copper Android banking samples and malicious email samples pointing to this domain, likely as part of the spreading campaign. A suspicious email from an account belonging to this same governmental entity distributing what seems to be AgentTesla suggests that at least one account was compromised by attackers to abuse recipients’ trust.

We also saw a Mexican governmental site hosting a veteran Windows banker family since the end of 2021, in what could also be an opportunistic attack. The malware was still present at the time of writing this report.

Ransomware

We didn't find many ransomware spreading cases, which should be considered good news.

A regional governmental domain in the Philippines was found hosting an AgentTesla sample by mid 2021. Attackers seem to have abused a vulnerability in the CMS to deploy their sample under a URL clearly used for social engineering, greatly increasing its potential to spread.

Targeted attacks and lateral movement

Under this category we found a few cases where either there were some indications the target was specifically chosen by attackers, or where we found malware typically used for targeted attacks. We cannot discard the possibility of some of them being the result of Red Teaming exercises, where security teams take the role of an adversary to improve defenders' infrastructure.

We believe a compromised Indonesian public hospital hosted Mimikatz in one of its subdomains – probably as part of attackers' deployment of lateral movement tools without triggering alarms.

In a similar situation, we found at least two Cobalt Strike samples hosted in a Sri Lankan governmental entity last July 2022 under a non-suspicious name. We believe it was likely deployed here as part of deploying attackers' lateral movement toolkit.

A Russian college hosted a malicious sample posed as an official thesis. The malware opened a DOCX with the thesis which then deployed a dropper at the same time. Another Russian educational entity hosted very similar malware, also dropping similar resources for the attack and opening an official-looking clean document during execution. We saw a different sample of the same family in a different educational institution in the Moscow region. We found yet another variant (first seen June 2021) opening a PDF instead of a document during execution, this time deployed in a governmental Russian site. A final variant of this attack was hosted in a Kazakhstan governmental site, opening a clean DOCX file during execution.

Webshells

Unfortunately, it is very hard to find and confirm active webshells for technical reasons. However, we can check if any governmental domain hosted any webshell at some point. Even when this does not confirm whether the site was indeed infected, we can confirm it was hosting malware, which is still a problem. This is an indicator attackers are abusing the governmental site as part of their attacking infrastructure, targeting the same or other targets.

Here there are some of our findings:

- **Webshells inside JPG files including PHP code.** This is a very old technique that should not work with modern PHP engines – unfortunately, it seems there are still some entities (three in Indonesia, one in Colombia) where we detected this problem. We also found an obfuscated webshell faking to be a GIF image in a Bangladeshian domain, a PHP webshell in a Mexican entity disguised as favicon.ico, and a foreign embassy in Tanzania with a PHP webshell with PNG extension, sending commands directly to the infected host.

- **An Indonesian government site hosted another simple passthru webshell, packed in a ZIP.** We found a US police department hosting the same obfuscated webshell under several URLs.

- **A Brazilian domain hosted a password-protected webshell.** Another Brazilian institution hosted a webshell from 2013, still active in 2021. This is not so uncommon given webshells are commonly reused.

- **PHP obfuscated webshells in an Ukrainian site.** Sometimes obfuscated webshells are distributed in ZIP files along a simple HTML file to hide the PHP, as in some Indonesian governmental sites. We found a second Ukrainian site hosting a version of the WSO webshell.

In addition to all the situations described, we found dozens of governmental websites that most likely had configuration issues, exposing sensitive information or allowing attackers to deploy phishing or malware through some subdomain or URL. In general, we find many situations where attackers, we believed, abused misconfiguration or vulnerabilities in CMSs. We also detected dozens of sites hosting either phishing malware or coinminers.

As a final note, we found several cases where hosted files were detected by AntiVirus, although we believe these are false positives. This can still be a concern for users of such sites.

Final thoughts

Malware and phishing attacks through government-related sites represent a potential major threat given the implicit trust these domains represent. Attackers including them as part of their infrastructure include both opportunistic and targeted attacks. We were able to find malware distributed from hundreds of government sites in more than 50 territories. Abused sites include phishing, distribution of malware, and potential compromised sites.

There are many sites that seem to lack regular maintenance or use vulnerable systems that allow attackers to host their malware. In some cases, it is likely the compromise occurred in an automated way without the attacker ever knowing they were abusing governmental institutions. In some other cases, we believe attackers used infected sites as part of their infrastructure to host malware temporarily as part of ongoing attacks. This has advantages for attackers such as minimizing the chance of triggering alarms, or creating more convincing social engineering schemes.

We suggest several ideas to minimize most common risks:

- Regularly update and maintain government web sites, especially content management systems (CMS), to address vulnerabilities.
- Actively monitor government infrastructure for anomalies, such as malware actively communicating with them or subdomains hosting files with malicious verdicts.
- Regularly scan all hosted files in government infrastructure, especially in subdomains and personal sites. Do not dismiss phishing, as it can be used in social engineering schemes.
- Assume traffic from trusted domains might be malicious, as the infrastructure can be used to host lateral movement tools or other advanced malicious toolsets.
- In case of finding anything suspicious, but especially in case of finding webshells or lateral movement tools in the infrastructure, assume compromise and consider a full investigation.

We believe, in many cases, that if these actions were taken, governmental sites would not be an easy victim. Other cases showed evidence of more advanced groups deploying their toolsets, which also should be considered when planning defenses based on allow/deny lists.

We consider that the examples found in this report should serve as a heads up towards better security practices when it comes to sensitive infrastructure. We hope examples are representative of different situations – however, we want to make clear this just scratches the surface and does not represent a full general overview.

Join the discussion @Virustotal

VIRUSTOTAL

Find out more at virustotal.com