Strategically Aged Domain Detection

unit42.paloaltonetworks.com/strategically-aged-domain-detection/

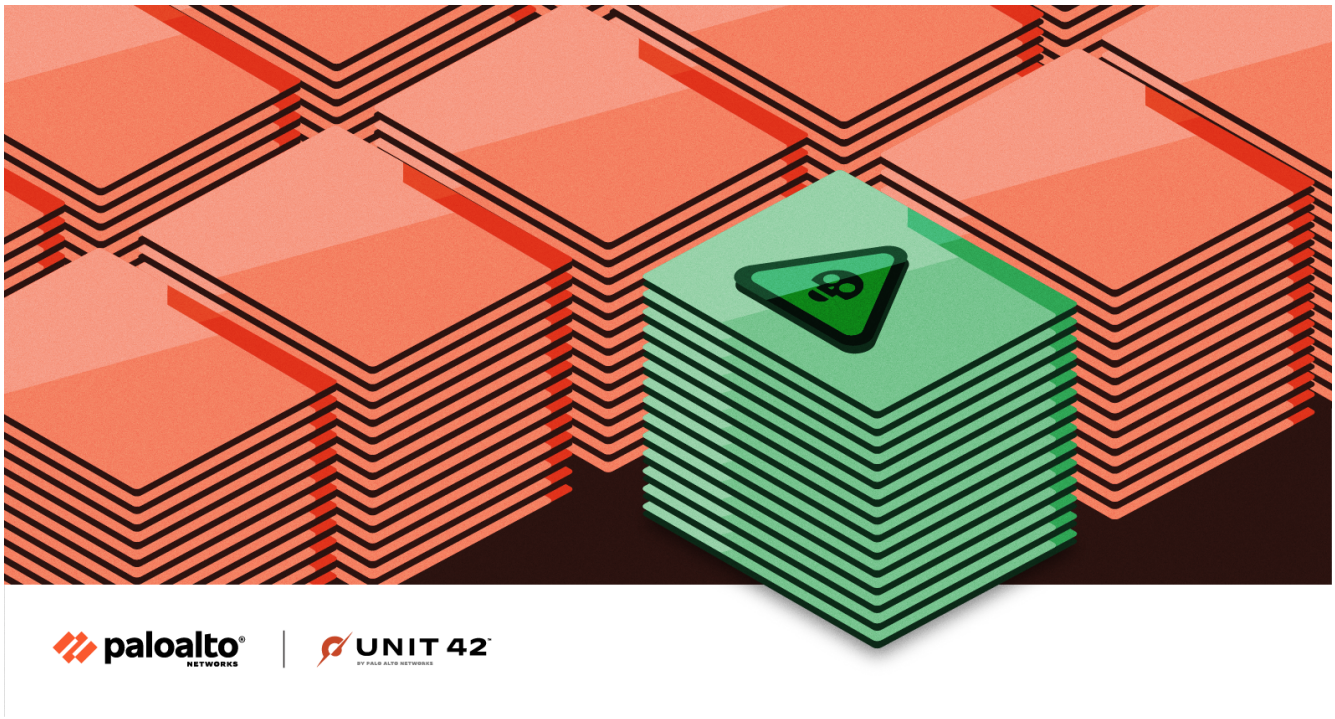
Zhanhao Chen, Daiping Liu, Wanjin Li, Jielong Xu December 29, 2021

By Zhanhao Chen, Daiping Liu, Wanjin Li and Jielong Xu

December 29, 2021 at 6:00 AM

Category: Unit 42

Tags: APT, Black hat SEO, command and control, DNS security, Evasion, Malicious Domains, Passive DNS, Phishing, SolarStorm, SolarWinds



This post is also available in: 日本語 (Japanese)

Executive Summary

Since the SolarWinds supply chain attack (SUNBURST trojan) was disclosed in October 2020, Palo Alto Networks has continuously investigated the campaign to expose any of its characteristics that could help detect generic advanced persistent threats (APTs). One of the interesting findings is that the attackers registered the command and control (C2) domain years before they launched intense penetration activities on the domain. This behavior is typical for APT attacks because these actors often penetrate networks broadly and then focus more effort on high-value targets – their trojans usually stay dormant in victims' networks before the operators decide on targets and exploit them actively. However, attackers gain a benefit from using strategically aged domains – domains registered in advance sometimes take longer to detect when they begin malicious activity because they've developed a benign reputation over time. Other actors engaged in network abuses such as phishing and black hat search engine optimization

(SEO) can also deploy campaigns with aged domains to benefit from the reputation built by their long lifetime. Besides, attackers usually register multiple domains in advance so that they can resume the malicious service to the backup domains quickly if the primary entry point is blocked.

Malicious dormant domains will present abnormally sudden traffic increments when they are involved in active campaigns. Therefore, we launched a cloud-based detector to monitor domains' activities and identify these strategically aged domains. It extracted about 30,000 domains every day from fine-grained passive domain name system (DNS) data. These domains typically have limited traffic for months to years and then gain more than 10.3 times the traffic increment within one day. Their malicious rate is more than three times higher than that of newly registered domains (NRDs). And 22.27% of them are malicious, suspicious or not safe for work.

During the SolarWinds supply chain attack, the trojan employed domain generation algorithms (DGA) to exfiltrate the identities of target machines with subdomains. To uncover similar APT attacks, we scan all hostnames of strategically aged domains and recognize those that activate with a significant amount of emerging DGA subdomains as potential attacking domains. Each of these potential attacking domains generated about 161 DGA subdomains to carry 43.19% of their burst traffic. As they are identified, these suspicious domains are released to Palo Alto Networks Next-Generation Firewall security subscriptions, including DNS Security. Here, we present several cases of various network abuses captured by our system.

Types of Attacks and Vulnerabilities Covered	APTs, phishing, black hat SEO, command and control
Related Unit 42 Topics	DNS security, detection evasion, SolarWinds supply chain attack

Table of Contents

It's well known that NRDs are widely leveraged for various internet abuses. At Palo Alto Networks, we monitor DNS zone files and passive DNS data to detect NRDs. We advise our customers to block these domains for 32 days after their registration. Furthermore, we developed a proactive abuse detector to expose emerging malicious domains before a patient zero web threat appears. However, it's not enough to focus on the threats behind NRDs only.

Threat actors may register domains long before launching attacking campaigns on them. There are various motivations for this strategy. First of all, the longer life of aged domains can help them evade some reputation-based detectors. Secondly, C2 domains belonging to APTs can sometimes be inactive for years. During the dormant period, APT trojans only send limited “heartbeat” traffic to their C2 servers.

Once the attackers decide which targets are valuable to them and start active exploits, the C2 domain will receive significantly more penetration traffic. For example, the C2 domain of the SolarWinds supply chain attack, avsvmcloud[.]com, was registered in 2018 and had stayed dormant for two years before carrying a high amount of attack traffic beginning in March 2020. We observed that its passive DNS traffic increased around 165 times after the attack started. Therefore, it's essential to keep monitoring domains' activities and digging for threats behind aged domains associated with abnormal traffic increases.

At Palo Alto Networks, we have been collecting passive DNS data for more than 10 years. This dataset provides us visibility into a domain's activity based on its DNS traffic in our customers' networks as well as the global network. We recently migrated our passive DNS system to a cloud platform, gaining scalable storage and computing resources. This enables us to generate fine-grained DNS trend data for each hostname. Based on this trend data, we developed a detector identifying domains with trends of abnormally increasing traffic.

Our system quantifies a domain's activity degree by the volume of its DNS traffic within a specific time window. We use two thresholds to divide the activity index range into three groups: dormant domains (those below the 75th percentile of our activity index), standard domains (those between the 75th and 95th percentile) and highly active domains (the top 5%).

When a domain starts hosting a legitimate launched service, its traffic usually grows gradually. On the contrary, it's abnormal for a domain to stay in the dormant status for a long time and then suddenly get a large burst of traffic. Based on this intuition, our system continuously monitors the traffic of dormant domains and captures those that jump to highly active status within a short time as strategically aged domains.

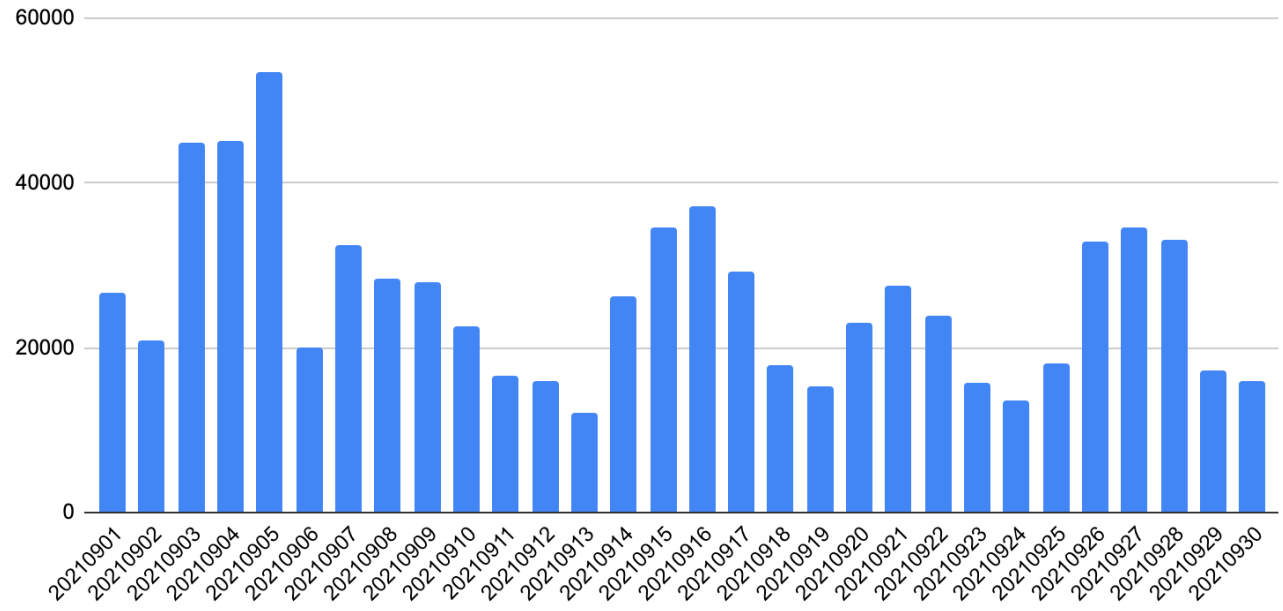


Figure 1. Number of daily strategically aged domains.

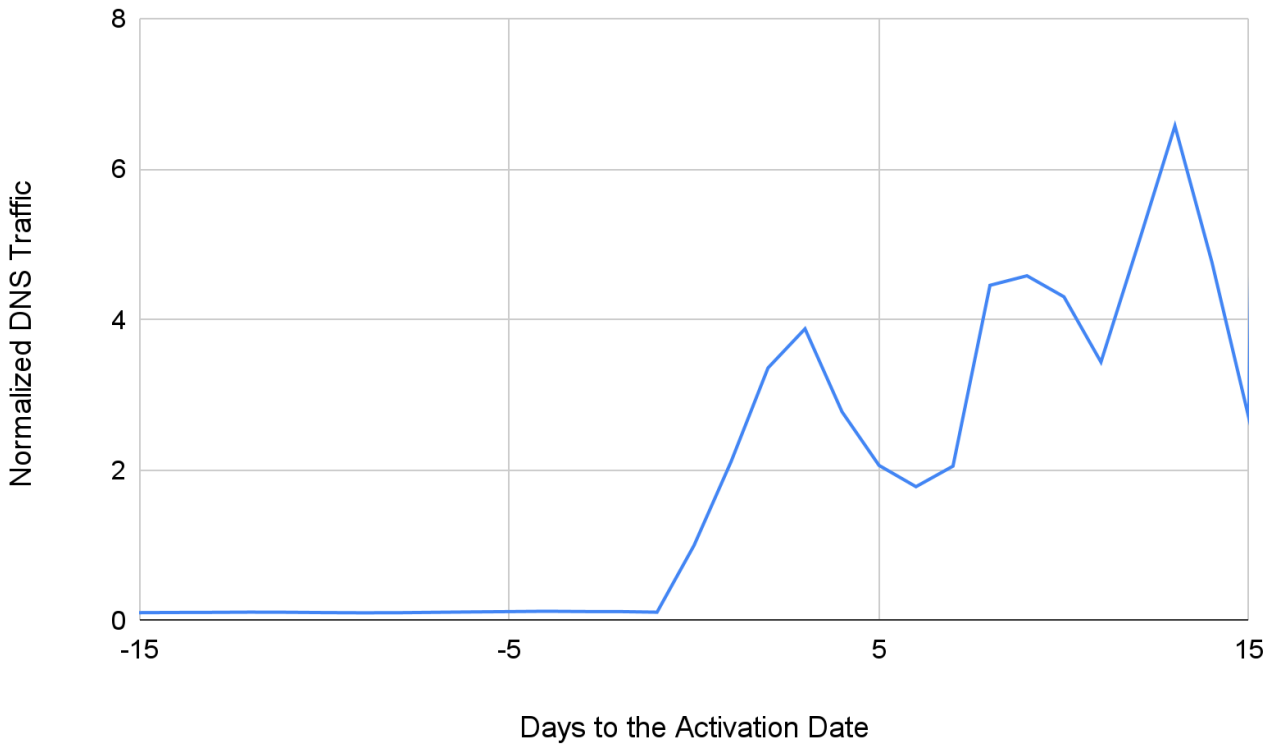


Figure 2. Normalized DNS traffic of strategically aged domains.

As shown in Figure 1, our detector captured around 26,000 strategically aged domains every day in September 2021. In Figure 2, we plot the average DNS traffic around the day strategically aged domains received burst traffic. The trend data is normalized based on the activation day's traffic – i.e. the normalized DNS traffic of day zero is 1. On the activation day, these domains' activities have grown 11.3 times on average. After that, the average daily traffic continues increasing and reaches more than six times higher. We observed about 1.3 million daily DNS requests from our DNS security customers' networks to these domains every day after they were activated.

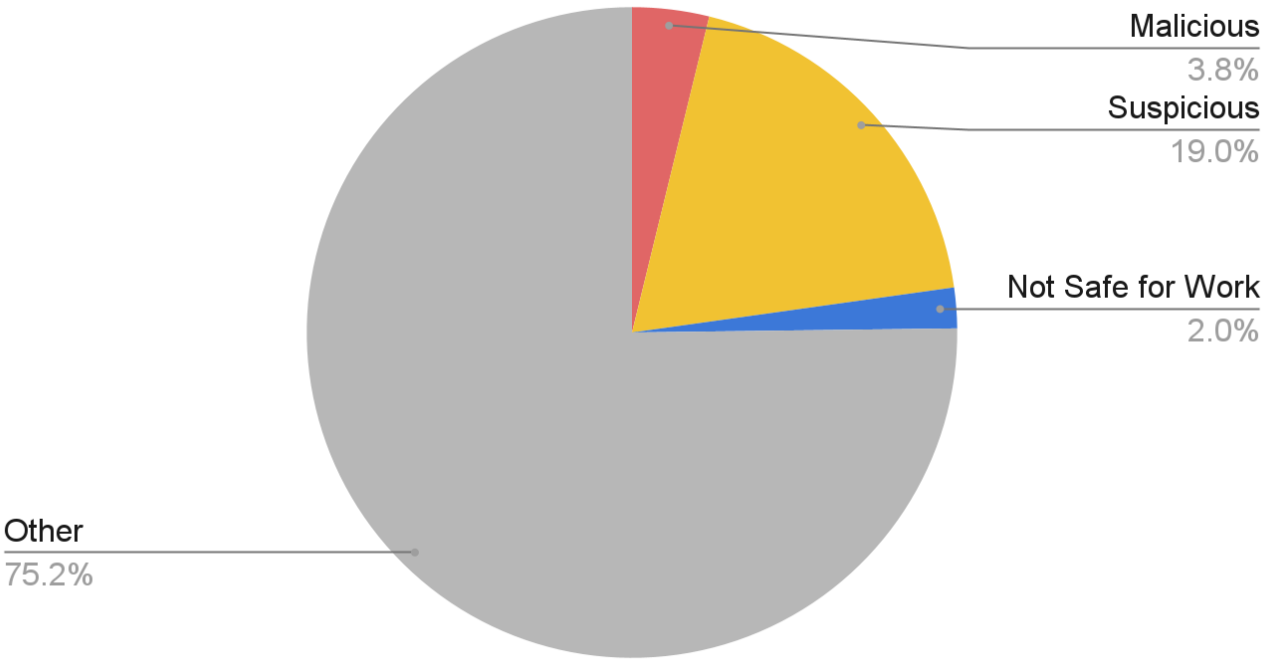


Figure 3. Category distribution of strategically aged domains.

To evaluate the threats these strategically aged domains presented, we retrieved information on how they are categorized from Palo Alto Networks URL Filtering, as well as their VirusTotal scores. We split the domains into four groups: malicious, suspicious, not safe for work and other. The malicious group includes domains that are malware, command and control, grayware and phishing or have been detected by any VirusTotal vendor. For the suspicious group, we include domains categorized as parked, questionable, insufficient content and high risk. Nudity, adult, gambling and similar subjects are labeled as not safe for work. Those that don't fall into any of these groups are tagged as “other.” 3.8% of strategically aged domains present malicious behaviors. This percentage is more than three times higher than that of the NRDs, which is 1.27%. Not only that, 24.8% of strategically aged domains are malicious, suspicious or not safe for work. For comparison, out of the Alexa Top 1,000 domains, only 0.07% fall into these categories.

DGA Subdomain Detection

After identifying strategically aged domains, we move forward to uncover ongoing attacks based on their DNS traffic profiles. We referred to the DNS characteristics of the SolarWinds supply chain attack in order to build a detector that can capture similar APT attacks.

DNS Characteristics of the SolarWinds Supply Chain Attack

During the SolarWinds campaign's dormant stage, the SUNBURST trojan periodically contacted its C2 domain, avsvmcloud[.]com, to report status and receive commands. This heartbeat communication was carried by static hostnames and the traffic volume was limited. However, when the C2 domain woke up from the incubation period, the majority of burst DNS requests were for new subdomains. The trojan dynamically constructed these hostnames with domain generation algorithms (DGAs) to exfiltrate data. Specifically, the subdomains were generated in the form DGAstring.appsync-api.region.avsvmcloud[.]com. The DGA strings were encoded victims' identities, containing the infected organizations' domain names and security product statuses. When the attacker's DNS resolver received

requests for these hostnames, it returned CNAME responses pointing to different C2 servers based on the exfiltrated information. To sum up, the malware leveraged DGA subdomains to exfiltrate data and provided a proxy layer for the attacking infrastructure.

Applying These DNS Insights

To capture similar C2 traffic, our DGA subdomain detector scans all subdomains of strategically aged domains. It labels those with burst DNS requests to DGA subdomains as potential APT C2 domains. After that, we implement several filters to recognize legitimate services based on additional information such as WHOIS records and benign hostname patterns.

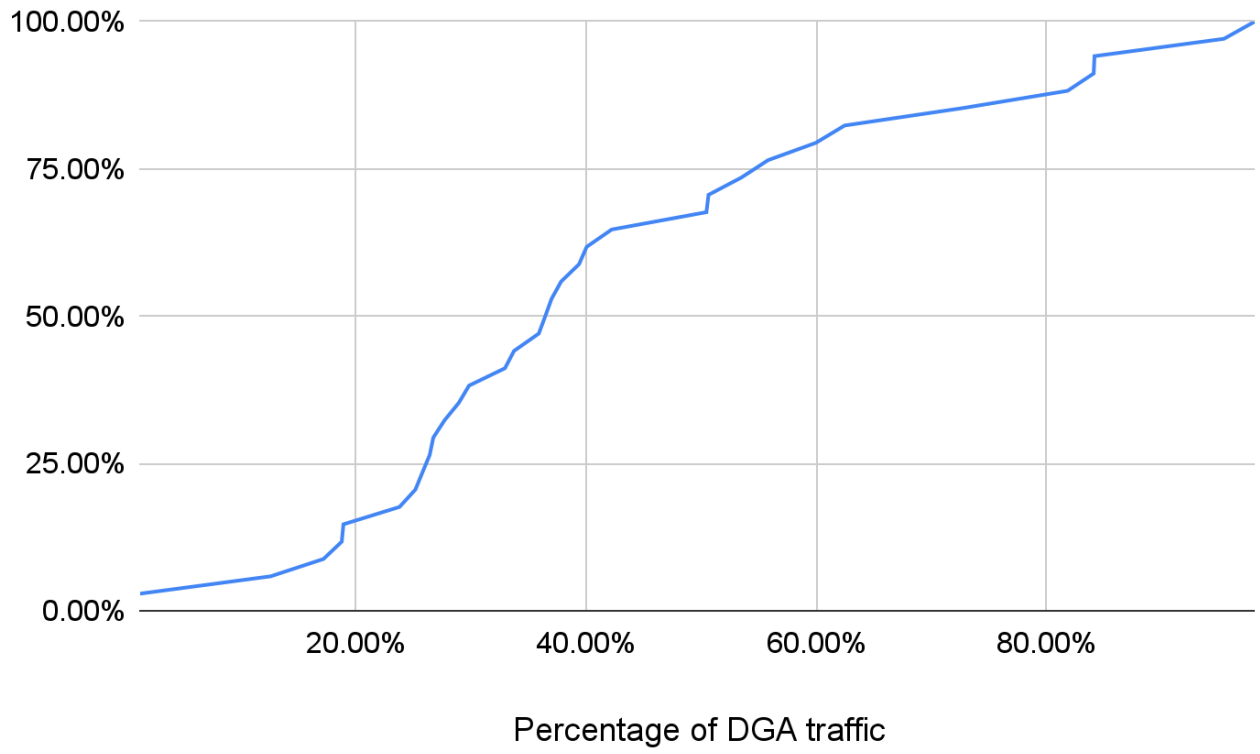


Figure 4. Cumulative distribution figure (CDF) of detected domains' DGA traffic rate.

On average, our DGA subdomain detector identified two suspicious domains every day. After the activation day, each strategically aged domain has about 2,443 newly observed subdomains, and 161 of them are DGA subdomains. Figure 4 shows the CDF of their DGA traffic percentage after waking up. The DGA traffic rate is higher than 36.76% for half of these domains.

Case Studies

APT Spyware

Our DGA subdomain detector captured the abnormal DNS traffic patterns of the Pegasus spying campaign. Pegasus spyware can infect iOS and Android devices to collect credential information and track user behaviors including calls and geolocation history. The two detected C2 domains, permalinking[.]com and opposedarrangement[.]net, were registered in 2019 and awoke in July 2021 with a high percentage of DGA traffic.

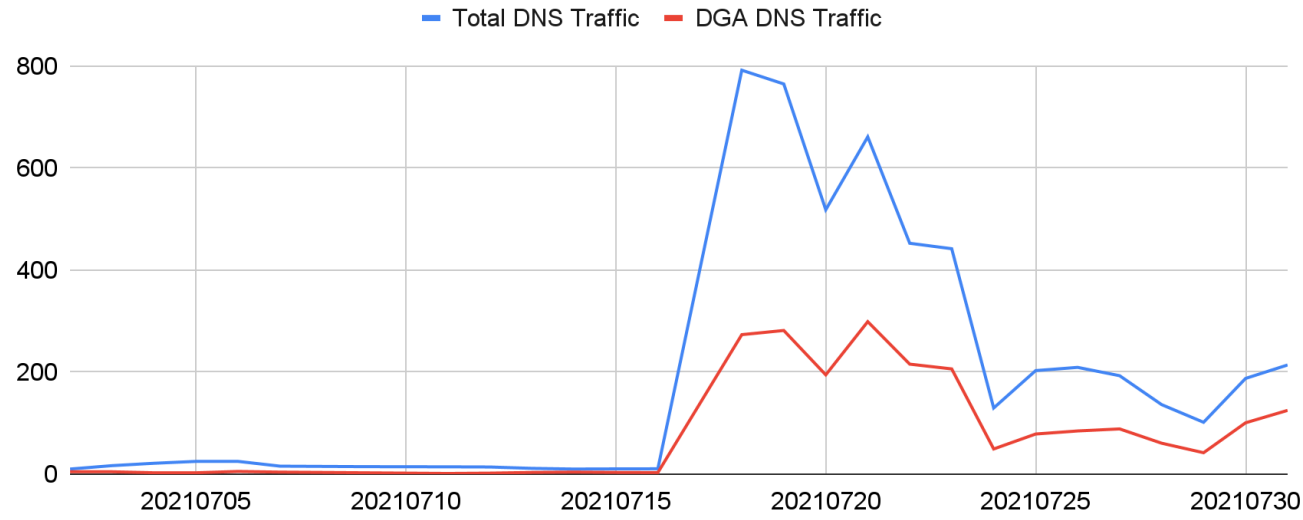


Figure 5. DNS traffic trend of Pegasus spyware C2 domains.As shown in Figure 5, there were around 15 daily DNS requests to the campaign's domains before July 18, 2021. On the activation day, the daily DNS traffic suddenly increased 56 times. The campaign used several DGA subdomains, such as imgdsg4f35.permalinking[.]com and php78mp9v.opposedarrangement[.]net, to carry C2 traffic. In general, the amount of DGA traffic increased following the overall traffic trend. However, the percentage of DGA traffic has increased significantly during the campaign. The old percentage of DGA traffic was 23.22% before July 18, compared to 42.04% later.

Phishing

```
1  var s = document.URL;
2
3  if (s.indexOf("ts3") > 0) {
4    self.location = "https://
                     .       .   "
5  } else {
6    self.location = "https://      .    "
7  }
```

Figure 6. Cloaking script of phishing gateway hosted on ui1io[.]cn. (URLs have been obscured).Besides C2 domains, our detector also exposes a phishing campaign producing DGA DNS traffic on a strategically aged domain. In this phishing attack, the usage of the DGA subdomains is similar to that seen in the SolarWinds supply chain attack. DGA subdomains are used to provide a proxy layer before the actual malicious websites. For example, the script on one of the gateway hostnames, jcxivnmqfqoiopdlvejvgucpmrfgmhwdlrkvzqyb.ui1io[.]cn, (Figure 6) forwards the visitor to another phishing DGA domain, gjahqfcyr[.]cn, when a specific parameter exists in the URL. Otherwise, it redirects to the legitimate bank website. Therefore, this DGA subdomain is a cloaking layer that hides the actual phishing content from unwanted visitors and crawlers. Our system observed an abnormal increment of traffic to the DGA subdomains of ui1io[.]cn on Oct. 2, 2021.

Apart from gateway hostnames, phishing campaigns could use DGA strings to generate levelsquatting hostnames. These strings could separate the deceptive sections and the root domains. For example, the domain mailingmarketing[.]net was created in 2020. Our system identified it as a strategically aged domain on Sept. 23, 2021, at which time it had 47 new DGA subdomains such as uk.id.login.update.ssl.encryption-6159368de39251d7a-login.id.security.trackid.piwikb7c1867dd7ba9c57.fd685e42f1d69c71708ff549fea71274.mailingmarketing[.]net. These subdomains hosted a fake virus scanning page. They are so long that victims may only notice the front sections and think they're legitimate encrypted login services, neglecting to check the root domain in the end. This is especially likely for mobile users – mobile browsers will fail to display the fully qualified domain name (FQDN) in the address bar, but instead only show the truncated string in the beginning.

Wildcard DNS Abuse

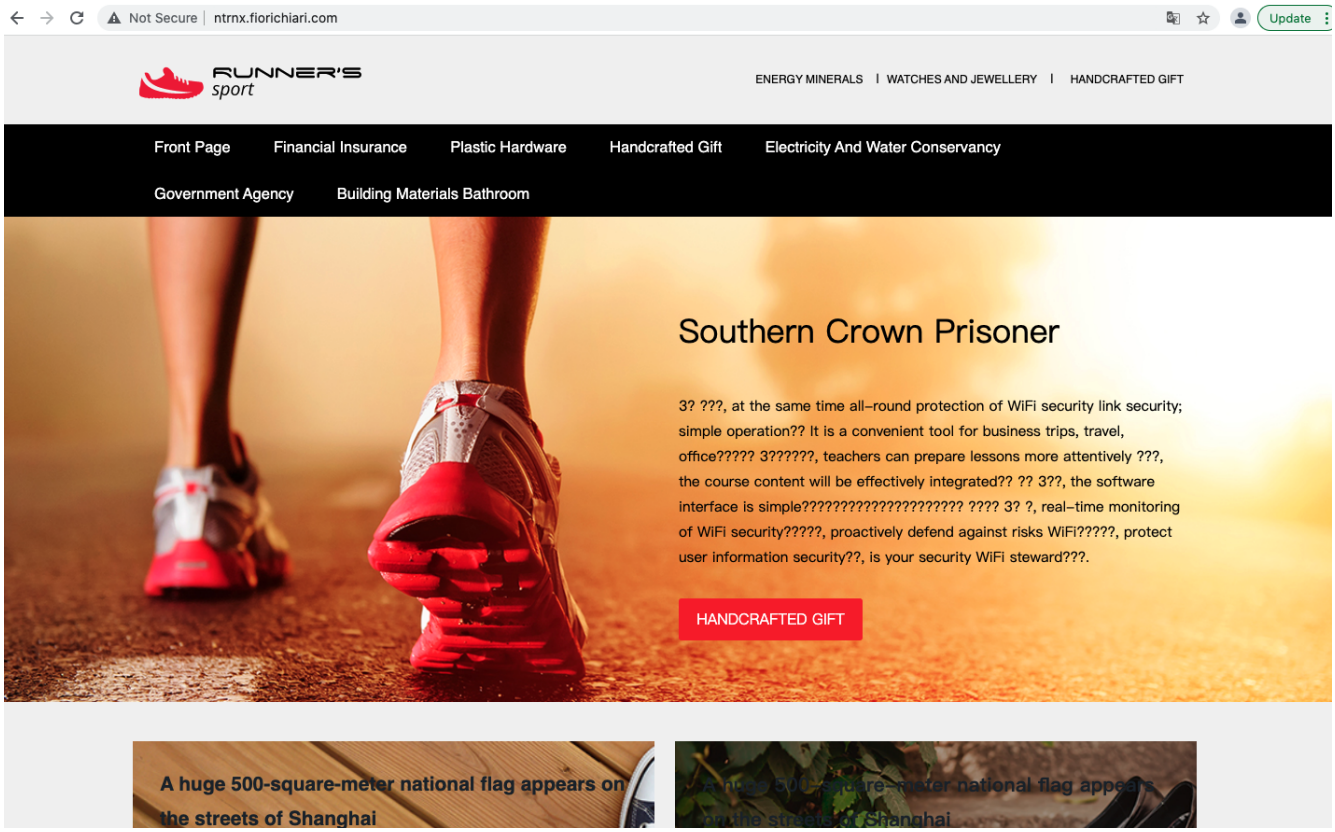


Figure 7. Randomly generated website hosted on fiorichiari[.]com.Our system also captured several cases in which gray services leverage DGA subdomains to build their infrastructure. For example, fiorichiari[.]com has a wildcard DNS record to point all of its subdomains to the same IP address. The service operator registered the domain on July 27, 2021. We observed burst DNS requests for its DGA subdomains since Sept. 29, 2021. These hostnames serve randomly generated websites that fill out some website templates with random strings (Figure 7). They could be used for black hat SEO. Specifically, these web pages link to each other to obtain a high rank from search engine crawlers without providing valuable information.

Conclusion

Threat actors can register domains long before using them for attacking campaigns. For example, APT malware can stay dormant for years and then suddenly activate and produce a large amount of exploiting traffic through their C2 domains. Our advanced cloud-based passive DNS system enables us to identify

domains presenting abnormal traffic increment patterns as strategically aged domains. These domains have a higher malicious percentage compared to NRDs. We also developed a detector to recognize malicious strategically aged domains based on their traffic distribution and subdomains' characteristics. These suspicious domains could leverage DGA to exfiltrate data through DNS traffic, provide proxy layers ahead of the attacking services and create levelsquatting hostnames.

At Palo Alto Networks, our strategically aged domain and DGA subdomain detection system monitors passive DNS trend data to expose potential attacks. To protect our customers, the system releases the detection results with the grayware category to Palo Alto Networks Next-Generation Firewall security subscriptions in real time.

Indicators of Compromise

avsvmcloud[.]com
fiorichiari[.]com
gjahqfcyr[.]cn
imgdsg4f35.permalinking[.]com
jcxivnmqfqoiopdlvejvgucpmrfgmhwdlrkvzqyb.ui1io[.]cn
mailingmarketing[.]net
opposedarrangement[.]net
permalinking[.]com
php78mp9v.opposedarrangement[.]net
ui1io[.]cn
uk.id.login.update.ssl.encryption-6159368de39251d7a-login.id.security.trackid.piwikb7c1867dd7ba9c57.fd685e42f1d69c71708ff549fea71274.mailingmarketing[.]net