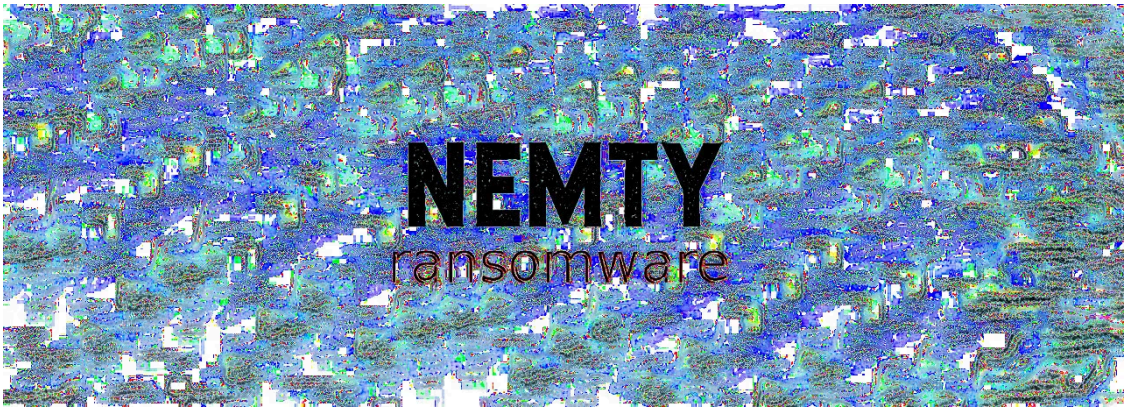
Nemty Ransomware Update Lets It Kill Processes and Services

By Ionut Ilascu

Published: 2019-09-14 · Archived: 2026-04-06 03:20:11 UTC

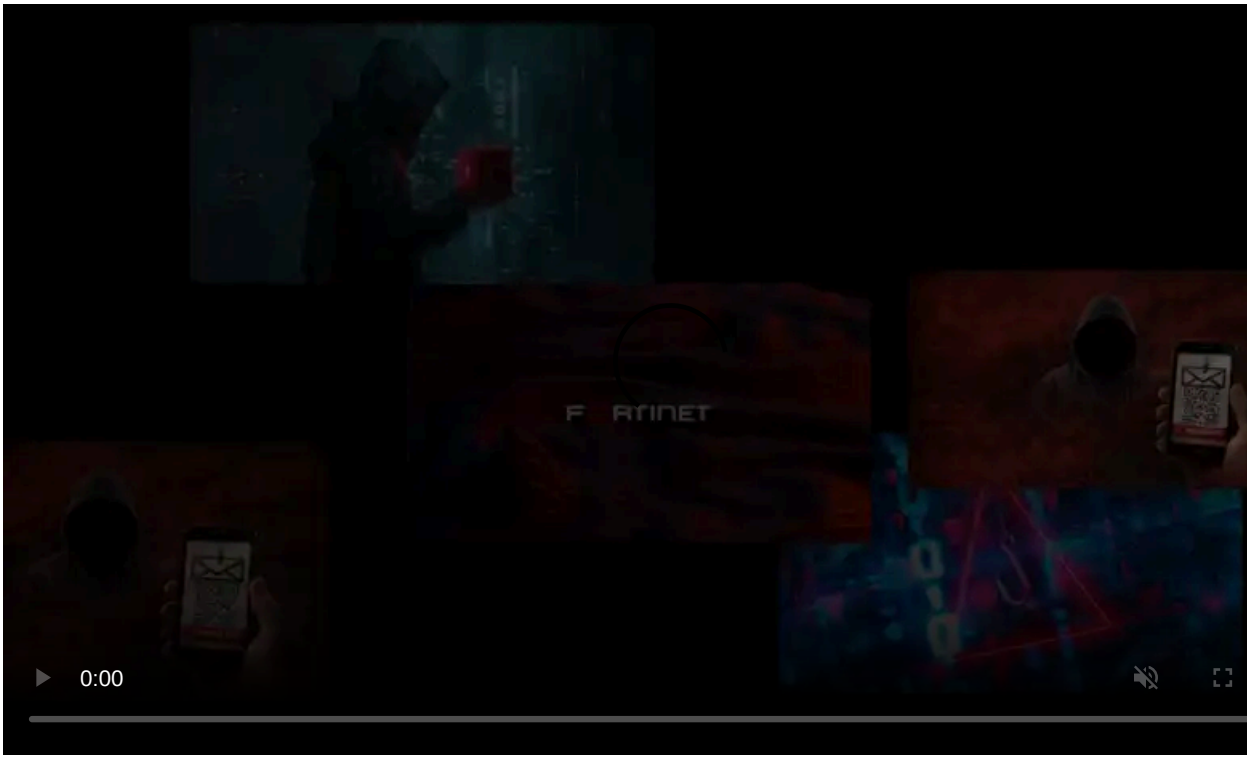


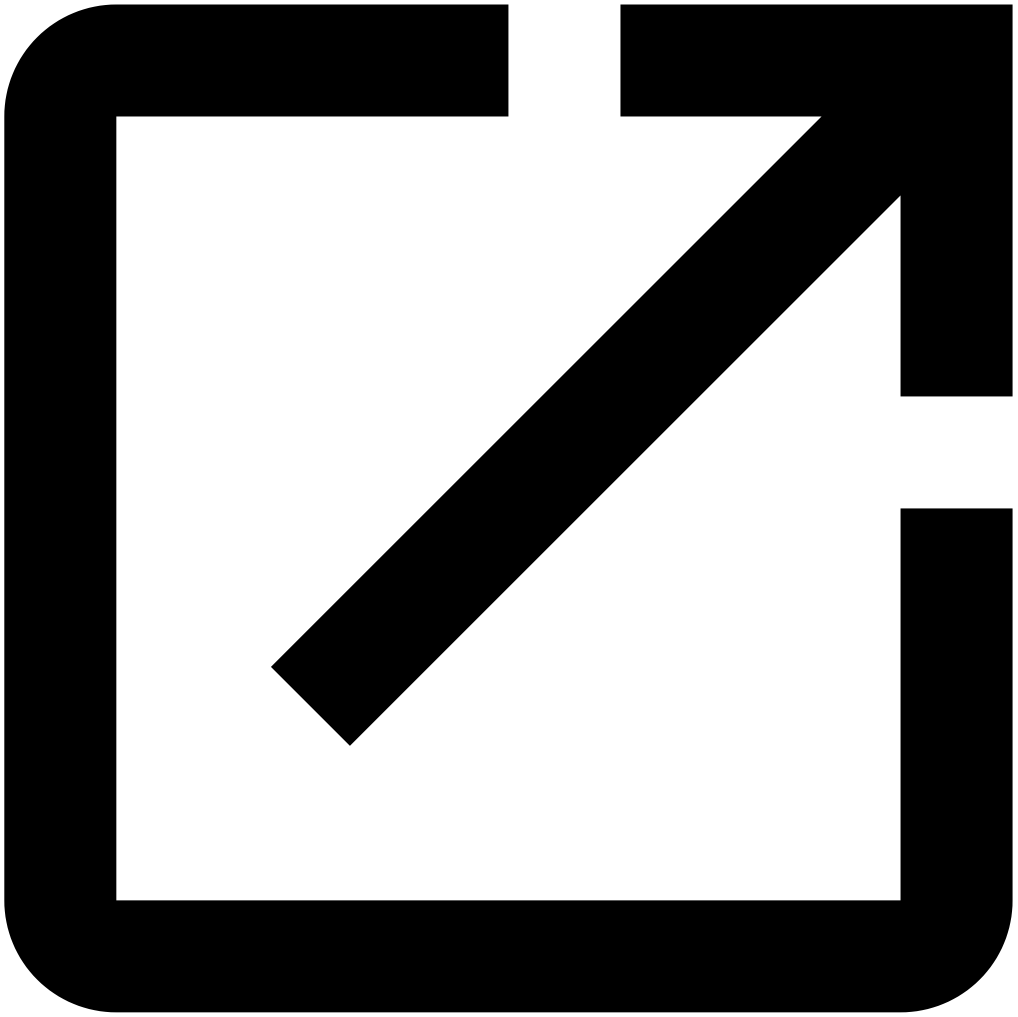
Nemty ransomware is under active development, although its version number may not show it. Its authors are clearly making efforts to make it a more efficient and sophisticated malware and it begins wider distribution.

The malware is new in the business and its cold reception in the ransomware underground community did not help it take off the way its administrators wanted.

Process and service killer

Despite making changes to the code, Nemty authors kept the same version number, shows an analysis from security researcher Vitali Kremez. The code, however, shows modifications that make the ransomware more aggressive in its actions.

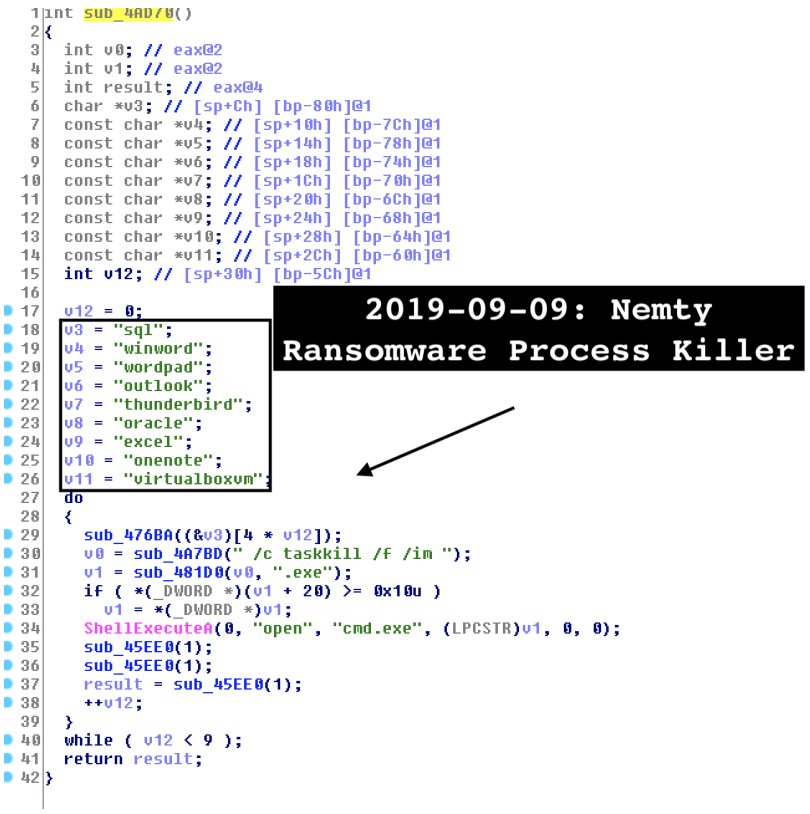

0:00



The researcher noticed that the latest version of the malware includes code for killing processes and services in order to encrypt files that are currently in use.

A look at Nemty's new code reveals a set of nine targeted processes, which include WordPad, Microsoft Word, Excel, Outlook Thunderbird email clients, SQL, and the VirtualBox software for running virtual machines.

With SQL and VirtualBox on the list, it gives us a clue that Nemty is targeting corporate victims.




```
int sub_4AD7B()
{
  int v0; // eax@2
  int v1; // eax@2
  int result; // eax@4
  char *v3; // [sp+Ch] [bp-80h]@1
  const char *v4; // [sp+10h] [bp-7Ch]@1
  const char *v5; // [sp+14h] [bp-78h]@1
  const char *v6; // [sp+18h] [bp-74h]@1
  const char *v7; // [sp+1Ch] [bp-70h]@1
  const char *v8; // [sp+20h] [bp-6Ch]@1
  const char *v9; // [sp+24h] [bp-68h]@1
  const char *v10; // [sp+28h] [bp-64h]@1
  const char *v11; // [sp+2Ch] [bp-60h]@1
  int v12; // [sp+30h] [bp-5Ch]@1

  v12 = 0;
  v3 = "sql";
  v4 = "winword";
  v5 = "wordpad";
  v6 = "outlook";
  v7 = "thunderbird";
  v8 = "oracle";
  v9 = "excel";
  v10 = "onenote";
  v11 = "virtualboxvm";
  do
  {
    sub_476BA((&v3)[4 * v12]);
    v0 = sub_4A7BD(" /c taskkill /f /im ");
    v1 = sub_481D0(v0, ".exe");
    if ( *(_DWORD *)(v1 + 20) >= 0x10u )
      v1 = *(_DWORD *)v1;
    ShellExecuteA(0, "open", "cmd.exe", (LPCSTR)v1, 0, 0);
    sub_45EE0(1);
    sub_45EE0(1);
    result = sub_45EE0(1);
    ++v12;
  }
  while ( v12 < 9 );
  return result;
}
```

List of terminated processes

More countries on the "no-no" list

Kremez also observed that the 'isRu' check has now extended to more countries. The full list now including Russia, Belarus, Kazakhstan, Tajikistan, Ukraine, Azerbaijan, Armenia, Kyrgyzstan, and Moldova, with the last four being the latest additions.

With an earlier version of the malware, 'isRU' did not make any difference for the encryption job and just marked those hosts to send system information to the command and control server. An update changed this and aborted encryption on computers positive for this check.

```
int isRu()
{
  const char *v0; // esi@9

  if ( (unsigned __int8)sub_487A3("Russia")
     || (unsigned __int8)sub_487A3("Belarus")
     || (unsigned __int8)sub_487A3("Kazakhstan")
     || (unsigned __int8)sub_487A3("Tajikistan")
     || (unsigned __int8)sub_487A3("Ukraine")
     || (unsigned __int8)sub_487A3("Azerbaijan")
     || (unsigned __int8)sub_487A3("Armenia")
     || (unsigned __int8)sub_487A3("Kyrgyzstan")
     || (v0 = "false", (unsigned __int8)sub_487A3("Moldova")) )
  {
    v0 = "true";
  }
  strlen(v0);
  return sub_47B55((void *)v0);
}
```

2019-09-09: Nemty Ransomware "isRu" Check Addition

Blacklisted countries

New distribution pipeline

One of the first versions of Nemty was seen distributed by RIG EK (exploit kit), while a more recent release, 1.4, spread through a fake PayPal page.

At the beginning of this week, a new release was observed by security researchers where they observed changes in the way victims are chosen and how the encryption process works.

The malware operators have a new distributor on their list, Radio EK, as found by nao_sec at the beginning of the week.

This is not a top-quality distributor, though, as the EK exploits a vulnerability in JScript and VBScript for Internet Explorer that Microsoft patched three years ago, the researcher told BleepingComputer.

Progress Telerik Fiddler Web Debugger - EKFiddle v.0.9.3.2

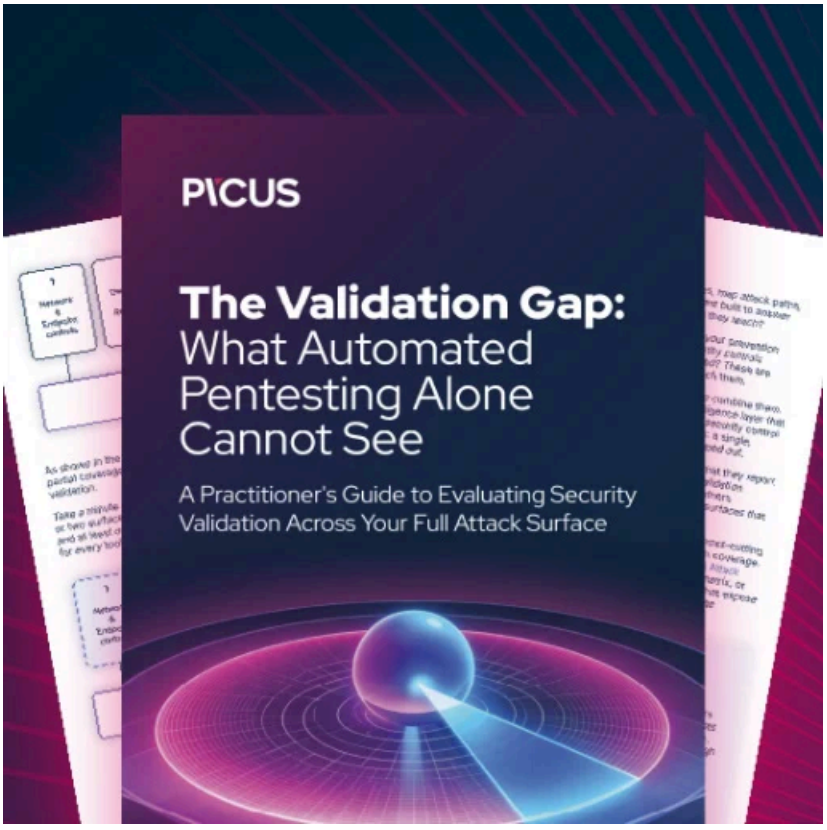
File Edit Rules Tools View Help Links

QuickSave UI mode VPN Proxy Import SAZ/PCAP Update/View Regexes Run Regexes Clear Markings WinConfig Rep

#	Result	Protocol	Host	URL	Body	Comments
1	301	HTTP	popcash.net	/world/go/216668/498903	162	
2	200	HTTP	ps.popcash.net	/go/216668/498903	426	
3	303	HTTP	ps.popcash.net	/ad/ad?p=216668&w=498903&t=878ebf2...	48	
4	200	HTTP	goodmany.site	/	3,550	Radio EK (CVE-2016-0189)
5	200	HTTPS	iplogger.com	/1IKvc	116	
6	200	HTTP	185.244.216.192	/images/9wywy.jpg	91,648	NEMTY Ransomware
7	200	HTTP	api.ipify.org	/	14	
8	200	HTTP	api.db-ip.com	/v2/free/[redacted]/countryName	5	
9	200	HTTPS	dist.torproject.org	/torbrowser/8.5.4/tor-win32-0.4.0.5.zip	5,594,336	

RadioEK in a malvertising campaign

Nemty may not enjoy much success at the moment but its authors seem to be putting in the energy to earn the respect of cybercriminals on ransomware forums and turn their malware into a lucrative business.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
