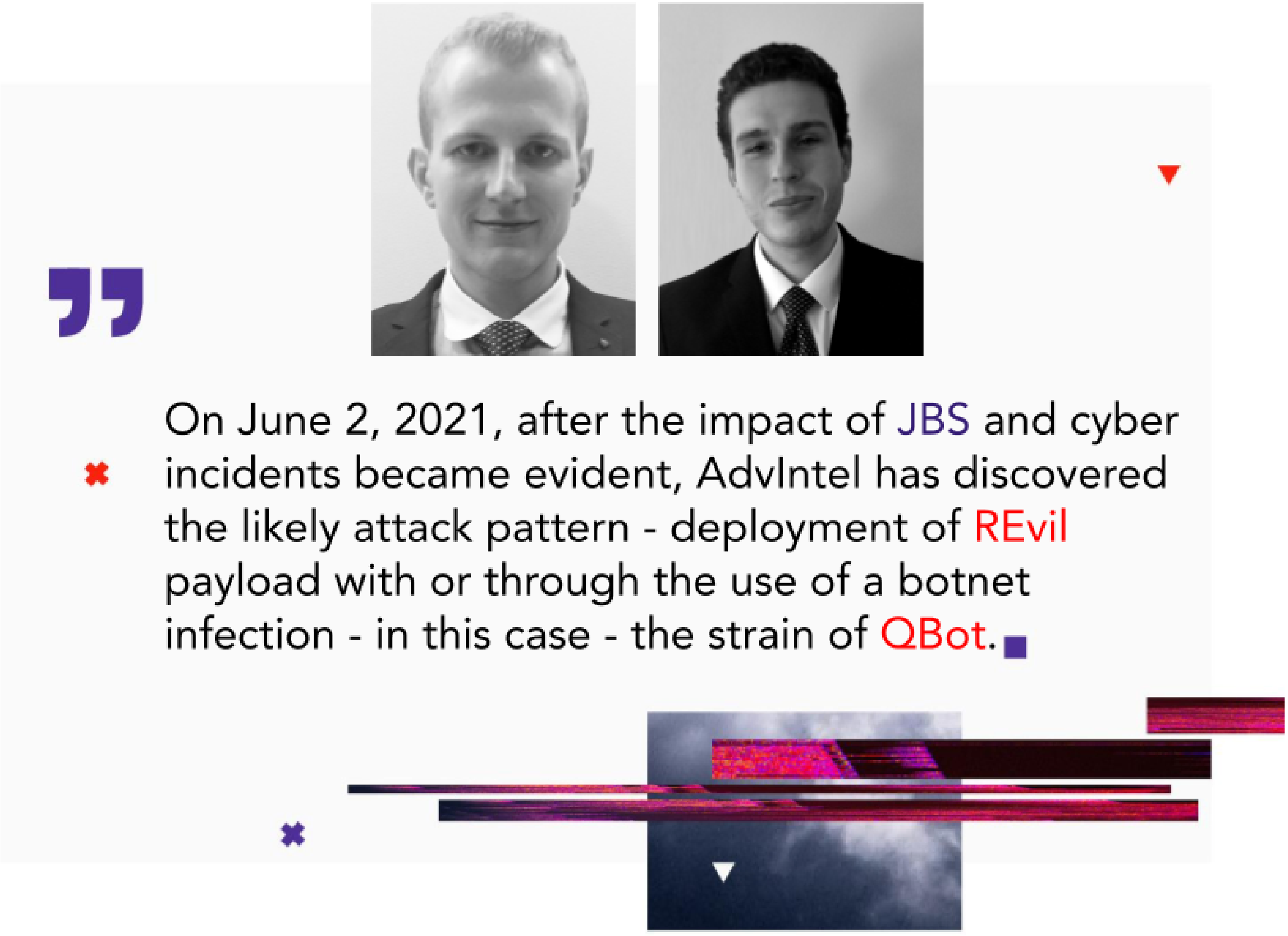
From QBot...with REvil Ransomware: Initial Attack Exposure of JBS

advanced-intel.com/post/from-qbot-with-revil-ransomware-initial-attack-exposure-of-jbs

AdvIntel June 7, 2021

- Jun 7, 2021
-
- 4 min read

Vitali Kremez & Yelisey Boguslavskiy



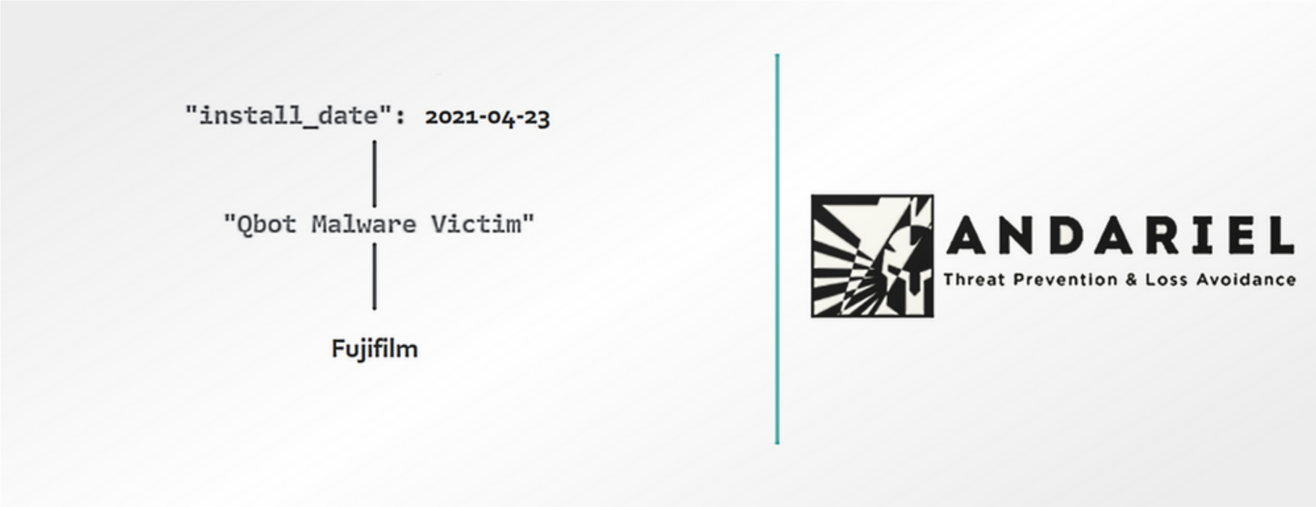
On June 2, 2021, after the impact of JBS and cyber incidents became evident, AdvIntel has discovered the likely attack pattern - deployment of REvil payload with or through the use of a botnet infection - in this case - the strain of QBot.

> At Advanced Intelligence, LLC we focus on providing *only* primary source proactive intelligence which supports our dual mission of providing threat prevention and loss avoidance solutions to our customer base.

Introduction

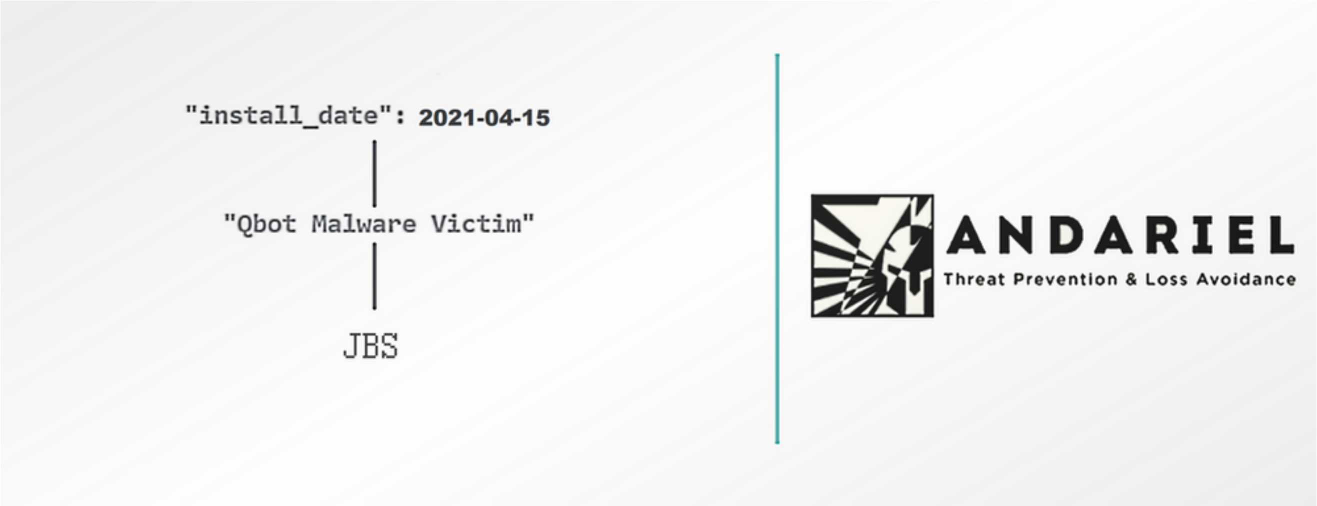
During the first week of June 2021, two major corporations were attacked by a ransomware group. JBS, the largest meat producer in the world, was hit on May 30, with the attack targeting the North American and Australian IT systems. Fujifilm, a Japanese multinational conglomerate was likely hit between June 1 and June second. Even though the two attacks and their victims, as well as jurisdictions, are radically different, a strong commonality suggests the same pattern and perpetrator - REvil gang possibly using the QBot malware to perform the initial infection operation.

On June 2, 2021, immediately after the first impact of both incidents became evident, AdvIntel has uniquely ***discovered*** the indicators which may suggest the likely attack pattern - deployment of ransomware payload with or through the use of a botnet infection - in this case - the strain of QBot.

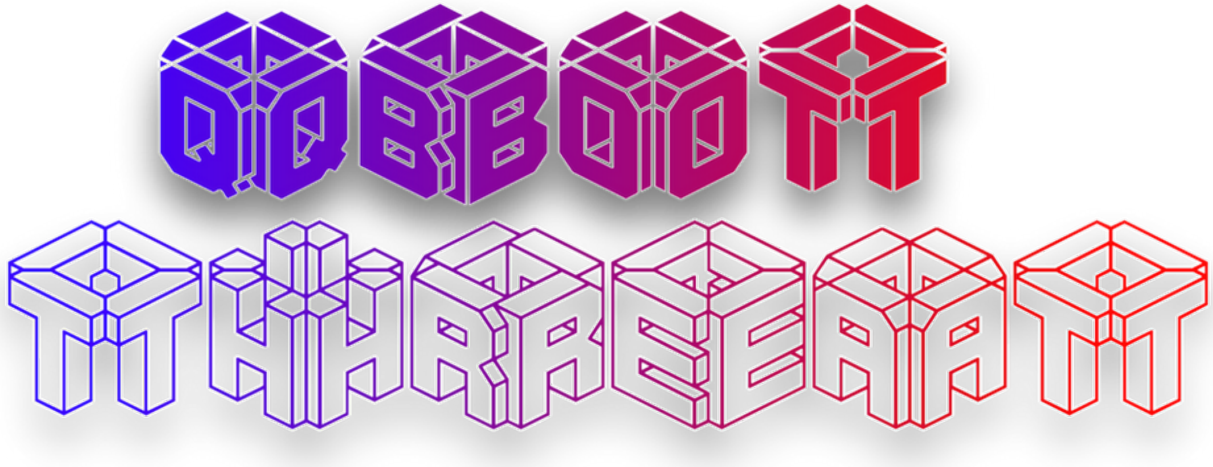

"install_date": 2021-04-23
"Qbot Malware Victim"
Fujifilm
ANDARIEL
Threat Prevention & Loss Avoidance

AdvIntel Andariel OMNI search reveals indicators of QBot presence prior to the attack for the Fujifilm incident

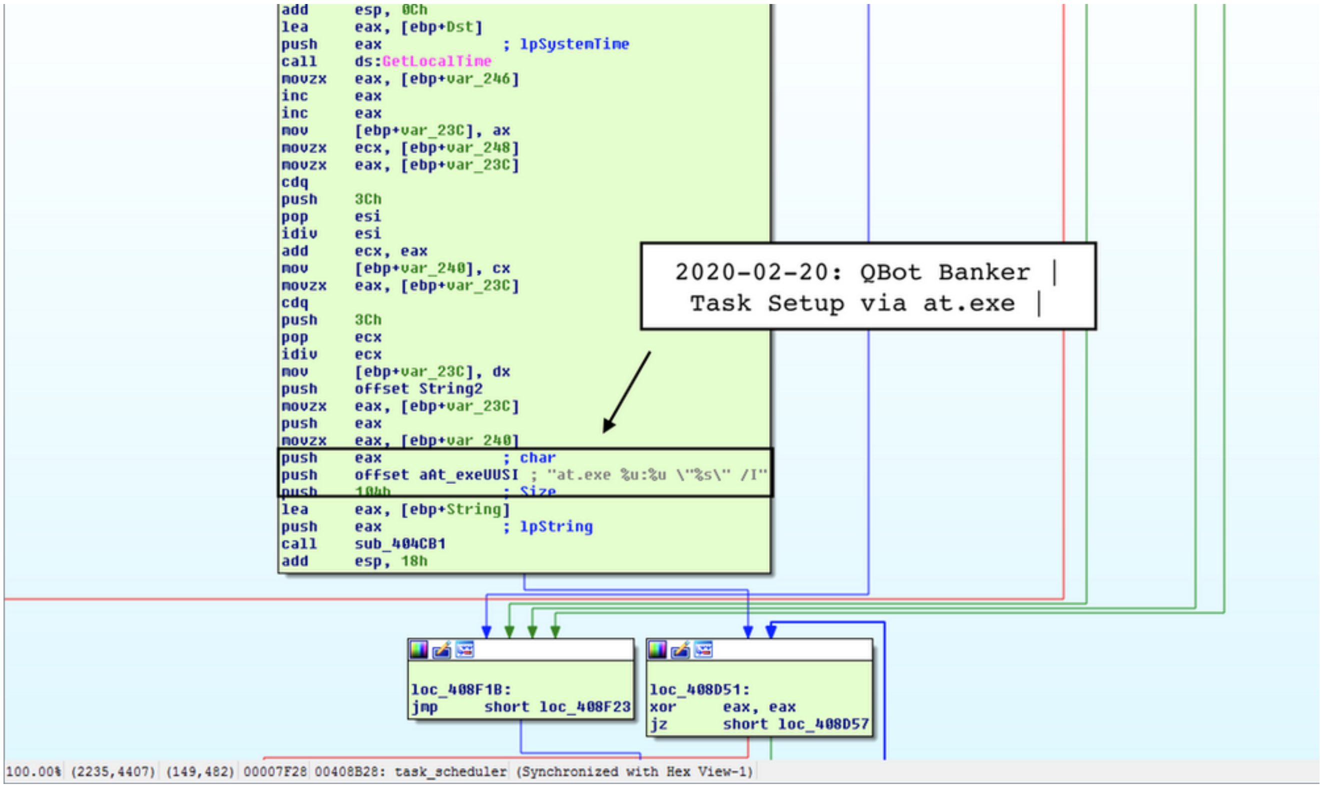
AdvIntel's Andariel unique ***OMNI*** Search feature that enables a holistic cross-platform and cross-source search across different underground domains, including botnets and vetted criminal infrastructures revealed the QBot IOCs for the fujifilm[.]com environments. Through this unique visibility into the threat actor infrastructures, we were able to observe advanced processes taking place in the networks of crime groups - REvil and QBot including an indication of QBot presence in Fujifilm networks for May 2021. Specifically, we have identified the QBot installation date as April 23, 2021.


"install_date": 2021-04-15
"Qbot Malware Victim"
JBS
ANDARIEL
Threat Prevention & Loss Avoidance

The same results were seen for the JBS - a QBot infection present at least since April 15, 2021.



QBot initially started as banking malware. Currently, the botnet has evolved into a sophisticated modular malware that possesses the ability to compromise sensitive information. The mechanics of the botnet includes the exploitation of hijacked email threads to begin the spread of infection. Well-designed email spam campaigns are then utilized to mass-distribute the infection in the victim networks; behavior also associated with Emotet. QBot group is considered a structured organization that is financially motivated. The group is assigned expert-level sophistication by AdvIntel's specialists. A network infection attributed to QBot automatically results in risks associated with future ransomware attacks, including REvil attacks.



```
add     esp, 0Ch
lea     eax, [ebp+Dst]
push    eax             ; lpSystemTime
call    ds:GetLocalTime
movzx   eax, [ebp+var_246]
inc     eax
inc     eax
mov     [ebp+var_23C], ax
movzx   ecx, [ebp+var_248]
movzx   eax, [ebp+var_23C]
cdq
push    3Ch
pop     esi
idiv    esi
add     ecx, eax
mov     [ebp+var_240], cx
movzx   eax, [ebp+var_23C]
cdq
push    3Ch
pop     ecx
idiv    ecx
mov     [ebp+var_23C], dx
push    offset String2
movzx   eax, [ebp+var_23C]
push    eax
movzx   eax, [ebp+var_240]
push    eax             ; char
push    offset aAt_exeUUSI ; "at.exe %u:%u \"%s\" /I"
push    104h            ; Size
lea     eax, [ebp+String]
push    eax             ; lpString
call    sub_404CB1
add     esp, 18h

loc_408F1B:
jmp     short loc_408F23

loc_408D51:
xor     eax, eax
jz      short loc_408D57

100.00% (2235,4407) (149,482) 00007F28 00408B28: task_scheduler (Synchronized with Hex View-1)
```

QBot's Task Scheduler Flow

We assess with a moderate-to-high level of confidence, that REvil and QBot closely cooperate and have joined efforts to target JBS and Fujifilm (JBS attack attribution to REvil has been already confirmed by the FBI and REvil themselves). The assessment is based on three indicators.

First, we have previously seen attacks in which QBot infection timing correlated with REvil attack timing. In other words, REvil’s attack - most often data leak followed the specific pattern of time after the initial QBot infection. For a sophisticated attack against a large target, it takes REvil two-to-three weeks to remain in the network. This exact timeframe between QBot infection and the REvil breach has been observed by AdvIntel while investigating REvil-related incidents.

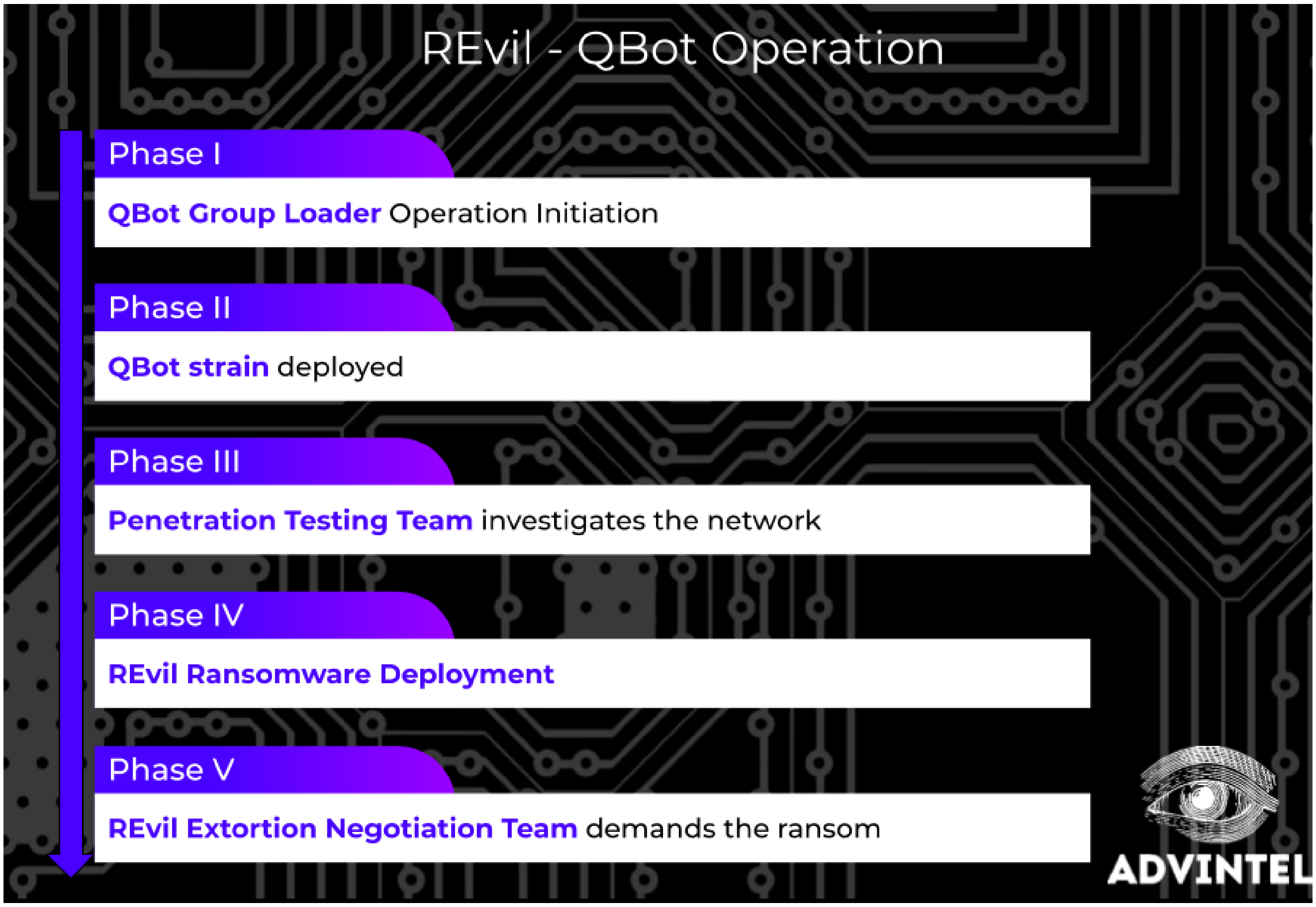
Second, our advanced underground community engagements and communication with threat actors directly related to REvil and QBot demonstrated certain evidence of cooperation between the two groups. Specifically, in the context of DarkSide - a known competitor of REvil succeeding in performing major cyberattacks initiated via botnet partnership with Zloader. The competition with DarkSide naturally leads to REvil’s agenda of building an elite botnet partnership.

> **...[i]t was a matter of time, when QBot loader group engages with REvil ransomware...**

Third, the TTPs and operational models of the two crime groups make this cooperation logical and natural. On the one hand, QBot as a botnet is known to build its business by engaging with as many top-tier ransomware groups as possible. A usual botnet group will have one partnership with a RaaS gang, sometimes two partnerships, but QBot differs from this pattern, as from the very beginning they were aiming at massive partnership expansions.

In other words, when other botnets only had one liaison on the ransomware side, QBot had many. For instance - Dridex had DopplePaymer; TrickBot botnet had Ryuk, Zloader had DarkSide, etc. At the same time, QBot had Egregor, ProLock, LockerGoga, Mount Locker, and other ransomware collectives. Therefore, it was a matter of time, when they engage with REvil.

At the same time, REvil, unlike other ransomware groups is known to diversify its attack tools. Usually, each ransomware group has its preferred tool, for instance, one infrastructural vulnerability, or one specific botnet. However, REvil aimed at covering as many attack surfaces as possible. Like many groups, they started with RDP exploitation, but they never stopped there. 2021 became REvil's year of rapid diversification. They announced investments in specialists in BlueKeep vulnerability, PulseVPN exploitation, Fortigate VPN exploitation. They have clearly expressed their interest in the novel Microsoft server CVEs, then in TrickBot malware, and then, finally, in a direct purchase of network access from underground.



REvil - QBot Operation

Phase I

QBot Group Loader Operation Initiation

Phase II

QBot strain deployed

Phase III

Penetration Testing Team investigates the network

Phase IV

REvil Ransomware Deployment

Phase V

REvil Extortion Negotiation Team demands the ransom

With such a pattern of two groups both aiming at approaching as many partners as possible and achieving the highest levels of diversification, it was a matter of time, when REvil and QBot would start cooperating. And of course, after the ransomware partnerships were banned on most of the underground forums, making it harder for them to communicate with the criminal community securing a partnership with another crime group becomes a priority for syndicates like REvil.

2021-07-06-AdvIntel-QBot-IOCs

.csv

Download CSV • 12KB