Cofense Intelligence™ Flash Alert

Report date: 2020-10-29

The Ryuk Threat: Why BazarBackdoor Matters Most

On October 28, media reports and U.S. Government (USG) notifications emerged regarding an active “credible” Ryuk ransomware threat targeting the U.S. Healthcare and Public Health sector. This was reportedly based on chatter observed in an online forum that allegedly included members of the group behind Ryuk. Cofense Intelligence™ is conducting an ongoing investigation into this threat, and we cannot evaluate the USG’s determination of this threat as credible, but we are taking this very seriously and have observed increased activity against the healthcare sector. We assess with high confidence that BazarBackdoor is the primary delivery mechanism currently used for Ryuk operations. Moreover, we have identified that similar phishing campaigns used to establish a foothold for Ryuk infections have targeted other sectors as well.

BazarBackdoor: Ryuk’s Inroad

Cofense Intelligence assesses that Ryuk operators typically wait until their preferred delivery mechanism is successfully deployed to an intended target prior to deploying Ryuk ransomware itself. Up until TrickBot’s disruption, Ryuk was most frequently delivered via TrickBot; however, our analysis indicates that the group behind Ryuk began leveraging BazarBackdoor to establish access to target systems in mid-September. This aligns closely with announcements that U.S. Cyber Command had taken action to disrupt TrickBot operations. In recent weeks, we assess with high confidence that BazarBackdoor has been Ryuk’s most predominant loader. With lower confidence, we assess this wave of Ryuk activity may be, in part, in retaliation for September’s TrickBot disruptions.

BazarBackdoor is a stealthy malware downloader that we assess is used by the same group as TrickBot. Typically, emails designed to appear as internal business communications are sent to victims within an organization, often with relevant employee names or positions. These emails usually contain a link, most often to a Google Docs page, though other well-known file hosting platforms have been used as well. The Google Docs page will then present a convincing image with another embedded link. This link is typically to a malicious executable hosted on a trusted platform such as Amazon AWS. This chain of legitimate services makes it difficult to detect and stop these campaigns.

Once in place on a victim’s computer, BazarBackdoor uses specialized network communications to avoid detection and to contact its command and control (C2) locations. Part of these communications involve DNS lookups for .bazar domains, which is the reason behind its Bazar name. These C2 locations also often serve as payload locations. After BazarBackdoor contacts its C2 center it will then collect additional information which the

threat actors can use to deliver customized reconnaissance tools, such as Cobalt Strike payloads. The threat actors can also choose to deliver other payloads such as Ryuk ransomware. The deployment of Ryuk ransomware is not automated, and therefore will not occur unless the threat actors decide the infected environment is a target.

Customers should pay special heed to any indications of BazarBackdoor compromise. Regardless of whether recent activity is in retaliation against TrickBot's disruption, what is clear is that recent efforts by multiple parties to cripple TrickBot seem to have been effective in transitioning the Ryuk actors to leveraging BazarBackdoor. We must be mindful that there are past connections between TrickBot activity and Emotet. While there is no direct evidence of current Emotet involvement in these campaigns, we cannot rule out future delivery of Ryuk via Emotet, given historical relationships between TrickBot and Emotet. As the TrickBot infrastructure appears to be in the process of restructuring, we assess that it may find use again as a delivery mechanism. As a network defender, all three malware families should be prioritized when searching for possible compromises, with the highest priority placed on detections of BazarBackdoor in the near future.

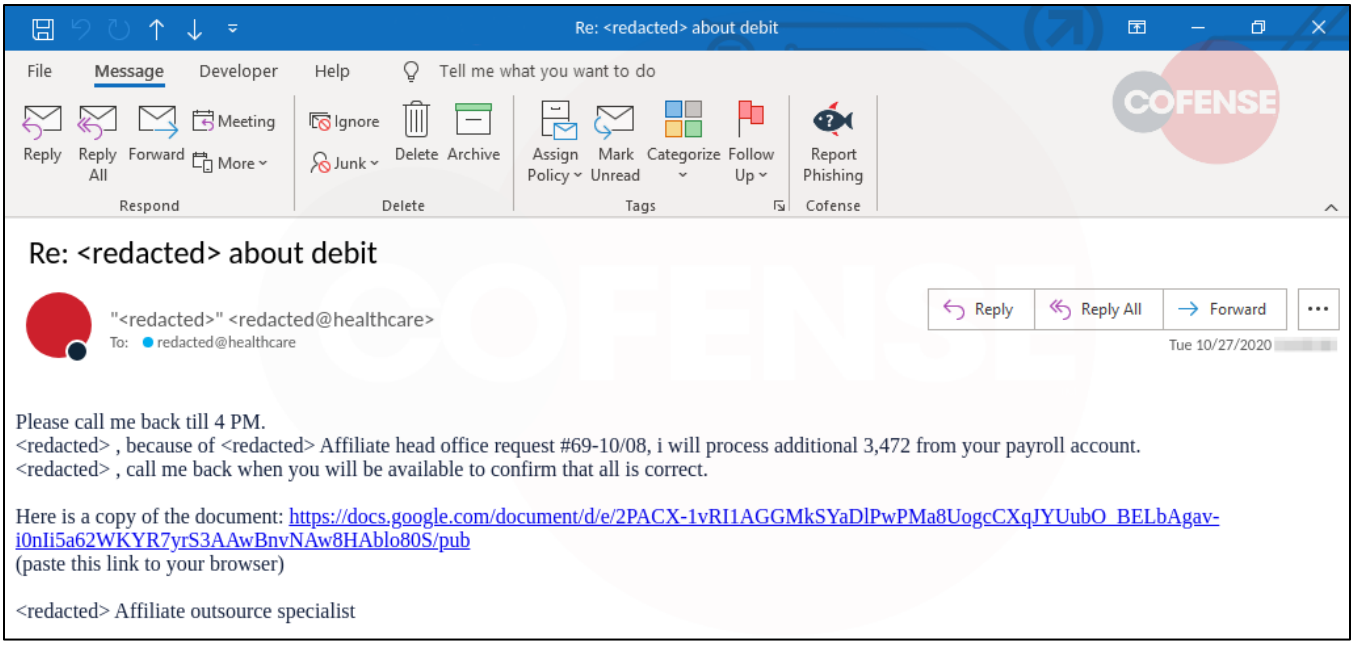

Figure 1: Common Phishing Example Delivering BazarBackdoor

The Phish

Cofense Intelligence has identified several campaigns, targeting multiple sectors, that share strong similarities to the phishing emails reportedly used as initial attack vectors in Ryuk campaigns, as outlined by FireEye. Two subject themes stand out across several industry verticals we have confirmed were targets of BazarBackdoor. These subjects relate A) to employment termination, almost always including the word "termination," or B) to payroll, almost always including the word "debit," as shown in Figure 1. While the subjects remain the same, we observed two separate download services: via Google Docs or Constant Contact. The following list highlights the

different industries we have confirmed were targeted by such campaigns. However, we cannot assess whether Ryuk operators intended to further infect these targets with Ryuk ransomware. This is due to the fact that it appears very likely that Ryuk operators have cast a wide net for potential infection vectors, and choose which successful footholds to manually interact with and leverage.

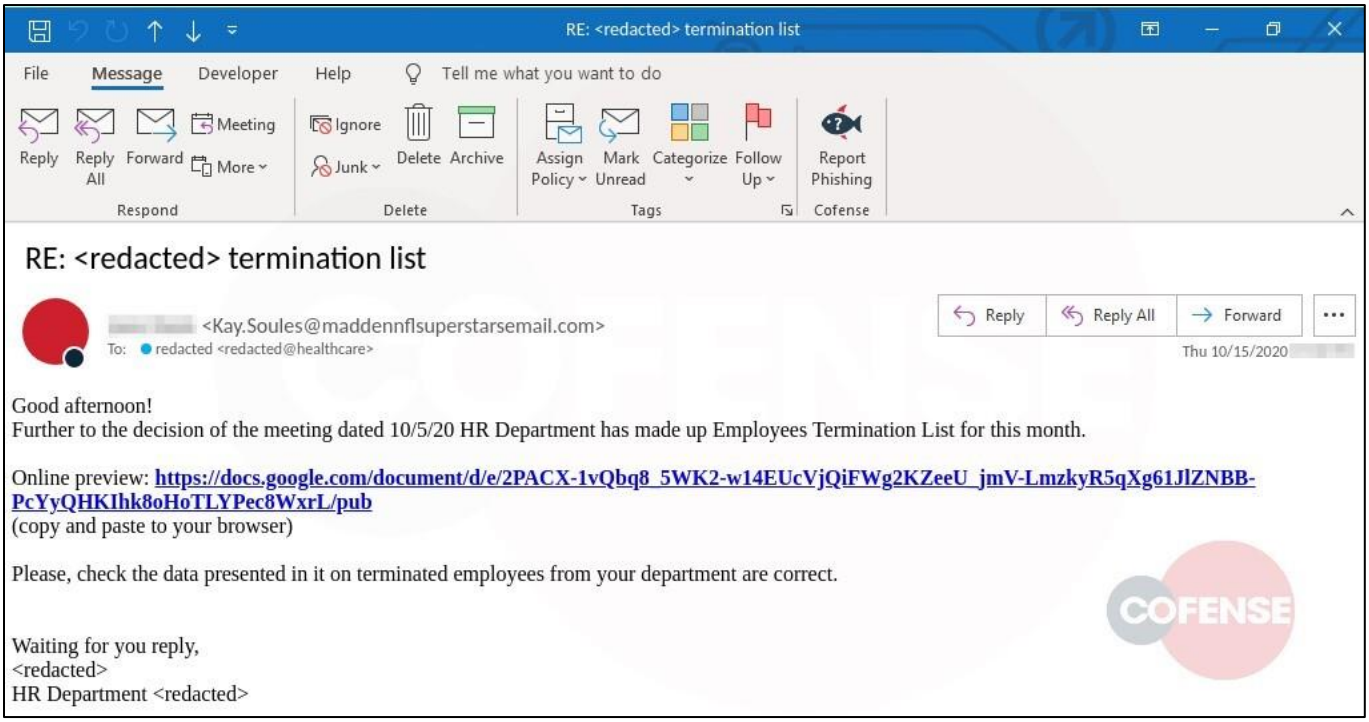

Figure 2: Termination List Phishing Example Delivering BazarBackdoor

It is worth noting, these campaigns began in mid-September, which corresponds with the timing of coordinated offensive operations to disrupt TrickBot. The sectors we have directly observed targeted in these campaigns include:

- Consumer Goods
- Energy
- Financial Services
- Healthcare
- Insurance
- Manufacturing
- Mining
- Professional Services
- Retail

Assessing the Threat

As of the early evening of October 29 (Eastern Daylight Time), there have not been reports of coordinated Ryuk attacks against U.S. hospitals. However, in recent weeks, there has certainly been an abundance of ransomware activity against the healthcare sector. It is not for us to say whether the stated time of the threat was off base, if there have been active successful countermeasures, or the flurry of reporting has deterred threat actors for now. It is possible they do not want to face such a well-guarded and prepared target-base. Still, we are confident that Ryuk operations have recently increased, and that other sectors have come into the crosshairs of potential future Ryuk operations. As such, it is our assessment that the threat should still be taken seriously.

Intelligence Customers can access all Intelligence IOCs tied to BazarBackdoor, TrickBot and Emotet via our API and on ThreatHQ. Below, you can find a table of relevant ATRs and Yara Rules associated with BazarBackdoor that can help your organization identify related emails should you be targeted.

Active Threat Reports: BazarBackdoor
71542
69892
67088
59926
56548
56336
55660
54647

Embedded URLs
hxxps://files[.]constantcontact[.]com/0d2efd83801/b5bc005e-db6a-43c8-a967-354f28e66b47[.]pdf
hxxps://files[.]constantcontact[.]com/0d2efd83801/ca3db959-6b1f-4df9-97b8-13772cbae8e4[.]pdf
hxxps://files[.]constantcontact[.]com/0d2efd83801/50f95d03-8af1-4396-ac84-d6a7f1212026[.]pdf
hxxps://files[.]constantcontact[.]com/0d2efd83801/786053b4-4dd9-418b-96bc-84fce4cd00e2[.]pdf
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQsr0bh2i5yJeikTd39t_QfodvTagGLUJNFbMXL_SPvj_x-Pl8WG8pqu6TqQykx9pRsTUvHEuthkWjE/pub
hxxps://download2020[.]xyz/xls7f283gd283/details_0710p[.]xls

hxxps://download2112[.]com/xls7f283gd283/details_0610p[.]xls
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vRHniSs5Zv8eT2oX5R6UMJPlmNCV_467IH7q9F_o9kwecObMgMt-p99b2ZKtfyXlPF-FdbfP4tArfHh/pub
hxxps://getfile24[.]com/xlsaf543f/details_0610s[.]xls
hxxps://getfile24[.]com/do[.]php
hxxps://download2112[.]com/do[.]php
hxxps://file2020[.]top/xlsaf543f/details_0710s[.]xls
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQI6-ZsmZthn9cMjphu3xI7yHO2XX-UGoWR5QdzQSY4hY-l0uPL-rVqMg7-Qtf1kjzwGJ0j9ZA3cSHf/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vTGg3jp69iZwWHQt_5iecBhuRO4TFrCqQGFH2SRnL7grlnhfFT_tvxB3b7MtJzcVCVKEjcoDET6WPZ1/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vSdRpDwxW652bF1MBskTuXdU21Vth9Igkq-wj-U2VyputfZw0eXOwEhB_tPm_OyXoqlwbv7JvwzOWN-/pub
hxxps://file2020[.]top/do[.]php
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vSl5CpqIn8TdaC2meLuo5O2_65-EG7BYAVWGpRfulpB6tcL9n4pWxSvNfMAbU9lCPgyPGJgc_mHl1N6/pub
hxxps://download2020[.]xyz/do[.]php
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQYIHCkjG5cyJ7LD20aBzlDCkuDspUXDzEHuUOZgceYCzhGuxTr3eS0CHwbgz4rB-z0-tc1PMG-G-Yf/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQihrkch2KlKXWyGgBLOOAUD8mtAQsbd33LRX382DLu29X3yXVqk0u5ZDyAQ1dxJoLAqT243vQA8zG6/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQWDqcUKNBnGdRrsYXzsk1yKMTevNW5TF_DvXV6KJkQcNS40pvDFIaTM3LLvROG270Vl_i-BfemLpeH/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vRcBIjcyojojwXhUnGOkJSHcufNT5dBBIeIjaDHJez8DNymddil19LHNH9m9txKwukWi9YweZmIYGbg/pub
hxxps://drive[.]google[.]com/uc?export=download&id=1S_a_Wl7U6HQqmIuHyTfutFCnllQVLDBO
hxxps://drive[.]google[.]com/uc?export=download&id=1YKT6EicsRHXPT0ecmt0y--9r-KdC0Vld
hxxps://drive[.]google[.]com/uc?export=download&confirm=no_antivirus&id=14VEtUrQbmx68Z742YYWaChtdGhejKHwr

hxxps://tackleadvisors[.]com/AnnualReport[.]exe
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQLld6CHo7dh7xjFodsvCIZoUgi1kChbFWe-HYCU-ehuLX5cW4S0YcIJagtcSIXrXEmLSNEFKkY2Ait/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQ2WZ6MMjC7qPmdB_EFnCyHskJ27X7rLc5pAbyxVJSpKKgcN3Q7j_b45gW6ueLliwJr4nEhVRwAM6AI/pub
hxxps://drive[.]google[.]com/uc?export=download&id=1UFjla7rs_X9BQw0K0EaylUH2DHkkCLRz
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQl8xkPTC5qcRYddleeD1wWjcL_--hdx0xmAEkwmmMnX6FXnPPI-eTnY7H4kljKVOeNuw_n16-YWE8v/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vRD18SMRqTb8GqUi9OeZbeMGgm3qAKfP94U-8CM7s8W1RlA6CmkpJ5ZZaqAzH07yA-rflst4tJiNJ5g/pub
hxxps://drive[.]google[.]com/uc?export=download&id=1QAxmrZowgewxFboMRcxJHfqB0ZnAiBZl
hxxps://drive[.]google[.]com/uc?export=download&id=1l2XzQBjyqq3adWQyRJMnHHuBoFKffue0
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQHuwqSVxsGvocUT5pUK9262gOvins1zEvXWnxjeJxqOpXzZhaKj-W6uthqmCN5N-VZW2TLOmW_0I5A/pub
hxxps://drive[.]google[.]com/uc?export=download&confirm=no_antivirus&id=1lGRZh86DPE59wL4OE07na0Q65YwuLWC9
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vSfT8MMEED7peY9YHyJ653d8JDvjd2EMkAiQgQ6_rEf0HoFffiKjK8-aKIBgxqXJi6wcqjOC5Mq6Pvn/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQpzU5su047G3V2PlnNgoGLChpX_QsCNaSJuarCKSHMISO4eq6vMJcrp0Jgwqwq4BAERrpgbpeiWHrO/pub
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vRuzQGE6Z2bu5LOPwejGkGqpJ3GQU2DThVj4BArRlqbIiQCt6Q976Ncydz0NPMXgFgP2kt7PMSHG46e/pub
hxxps://drive[.]google[.]com/uc?export=download&confirm=no_antivirus&id=1qM01ivzPpKAuwNCbRBRoI2TtV0HkrvJ9
hxxps://docs[.]google[.]com/document/d/e/2PACX-1vRKjSRJ8GpqWEk4fINOr4nV31P9VWQ868hfqEZyNb5WhVO9Of_0AFavdwEsmlzu2LRJuNdEEA4ZYlDg/pub
hxxp://195[.]123[.]241[.]154/fonts[.]php

hxxps://docs[.]google[.]com/document/d/e/2PACX-1vQorNnj4QnVfP_DFo6G3znMTvbPUnbkWH4QnGmIHAdDcHOCmYjqhsaI0NyUaTEJDQFPp3ZMMaowisPz/pub
hxxp://docs[.]google[.]com/document/d/e/2PACX-1vRR--Nv_XxP5TyJpc0w4eNrNfWtVlHnMt5nK33ZHtylR5Dl4BXijSwb722XWQXLJObB2gAziS77ZUIM/pub
hxxp://195[.]123[.]232[.]163/abcf563px3i[.]php
hxxp://docs[.]google[.]com/document/d/e/2PACX-1vQ5-Kr-eOjPFeWs-MZR1Flspv0kBIQiQDeUyuTcXHHkZlEK6jDQDJnsIQqkAXQ9iRpIo5cRg73d7ztK/pub
hxxp://docs[.]google[.]com/document/d/e/2PACX-1vQM6VfkT7hU3MM8KJQgY7E9BnnnMVuWLws1Sl0cGPh6a_9Me8u2YsWx_j4bL5iEHQyoMSMo54twwhV1/pub
hxxp://docs[.]google[.]com/document/d/e/2PACX-1vQg_6O82GtGQVvwG0296E3SefhAcxhkWskkdVES3r-x774F3-kY4a6hQuYJC5SgKj3lOA2mrPx6BxGx/pub

BazarBackdoor File	MD5 Hash
Document3-90.exe	3826f8176445cc4291287f8aad28bb53
Report10-9.exe	240bf9b477fe3d977acbb2726f0f12b5
1.exe	b9e7cdd63db7ff765efeaabd0a85ca59
2.exe	d3965ca520a87fc3ad3a874bb0bf118c
AnnualReport.exe	ff9976d675cc1679b0b6e15323010dbf
AnnualReport.exe	49c3639ad3cd29473e0bd047bcef8a64
Document_Print.exe	925d730ddb4304a4bde4dfaeabb5c7b9
Document-Preview.exe	40b17d4ca83f079cf6b2b09d7a7fd839
t99.exe	df249304643531adb536eba89691ec91
PreviewDoc.exe	a41429f7dbecfb76e6b7534afbeb4f74
Preview.exe	9f00d78f2e8e4523773a264f85be1c02
Preview.exe	5f64cc672ea13388797599b40a62d9be
putty.exe	006f8bd0cd7e820705dec7bb3a7a7cf5
XColorPickerXPTest.exe	cd6b9af8db078afe074b12a4fd0a5869

BazarBackdoor File	MD5 Hash
PDOKGLWEER.exe	135f68e708cc04e362703ad71be5f620
v152.exe	d55ec134a3046f289d9ebfdba1e98775

BazarBackdoor Command
hxxps://107[.]155[.]137[.]18/api/v150
hxxps://107[.]155[.]137[.]18/api/v152
hxxps://164[.]132[.]76[.]76/api/v12
hxxps://164[.]68[.]107[.]165/api/v10
hxxps://164[.]68[.]107[.]165/api/v12
hxxps://185[.]99[.]2[.]196/api/v12
hxxps://194[.]5[.]249[.]156/api/v10
hxxps://195[.]123[.]241[.]175/api/v153
hxxps://195[.]123[.]241[.]194/api/v153
hxxps://212[.]22[.]70[.]4/api/v12
hxxps://31[.]214[.]240[.]203/api/v150
hxxps://31[.]214[.]240[.]203/api/v152
hxxps://35[.]164[.]230[.]208/link/s
hxxps://45[.]148[.]10[.]190/api/v150
hxxps://45[.]148[.]10[.]190/api/v152
hxxps://5[.]182[.]210[.]145/api/v10
hxxps://5[.]182[.]210[.]145/api/v12
hxxps://54[.]89[.]230[.]95/rest/t
hxxps://68[.]183[.]214[.]30/api/v12
hxxps://82[.]146[.]37[.]128/api/v150
hxxps://82[.]146[.]37[.]128/api/v152

hxxps://82[.]146[.]37[.]128/api/v153
hxxps://82[.]146[.]37[.]128/api/v154
hxxps://85[.]143[.]221[.]85/api/v100
hxxps://85[.]143[.]221[.]85/api/v150
hxxps://85[.]143[.]221[.]85/api/v152
hxxps://85[.]143[.]221[.]85/api/v98
hxxps://86[.]104[.]194[.]77/api/v10
hxxps://86[.]104[.]194[.]77/api/v12
hxxps://bubl6g[.]com:443/api/v202
hxxps://bubl6g[.]com:443/api/v204
hxxps://grumhit[.]com/z/report
hxxps://onevdg[.]com/link/s

Yara Rules for Campaign Detection

```
rule PM_Intel_Ryuk_Payload_1029201 {
meta:
  description = "EDR rule for detecting Ryuk ransomware main payload"
strings:
  $ = ".RYK" wide nocase
$ = "RyukReadMe.html" wide nocase
$ = "UNIQUE_ID_DO_NOT_REMOVE" wide nocase
$ = "\\users\\Public\\finish" wide nocase
$ = "\\users\\Public\\sys" wide nocase
$ = "\\Documents and Settings\\Default User\\finish" wide nocase
$ = "\\Documents and Settings\\Default User\\sys" wide nocase
condition:
  uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and all of
them
}
```

```
rule crime_win64_backdoor_bazarbackdoor1 {
meta:
 description = "Detects BazarBackdoor injected 64-bit malware"
 author = "@VK_Intel"
 reference = "https://twitter.com/pancak3lullz/status/1252303608747565057"
 tlp = "white"
 date = "2020-04-24"
strings:
 $str1 = "%id%"
 $str2 = "%d"
 $start = { 48 ?? ?? ?? ?? 57 48 83 ec 30 b9 01 00 00 00 e8 ?? ?? ?? ?? 84 c0 0f ?? ?? ?? ?? ?? 40 32 ff 40 ?? ?? ?? ?? e8 ?? ?? ?? ?? 8a d8 8b ?? ?? ?? ?? ?? 83 f9 01 0f ?? ?? ?? ?? ?? 85 c9 75 ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? e8 ?? ?? ?? ?? 85 c0 74 ?? b8 ff 00 00 00 e9 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? e8 ?? ?? ?? ?? c7 ?? ?? ?? ?? ?? ?? ?? ?? ?? eb ?? 40 b7 01 40 ?? ?? ?? ?? 8a cb e8 ?? ?? ?? ?? e8 ?? ?? ?? ?? 48 8b d8 48 ?? ?? ?? 74 ??}
 $server = {40 53 48 83 ec 20 48 8b d9 e8 ?? ?? ?? ?? 85 c0 75 ?? 0f ?? ?? ?? ?? ?? ?? 66 83 f8 50 74 ?? b9 bb 01 00 00 66 3b c1 74 ?? a8 01 74 ?? 48 8b cb e8 ?? ?? ?? ?? 84 c0 75 ?? 48 8b cb e8 ?? ?? ?? ?? b8 f6 ff ff ff eb ?? 33 c0 48 83 c4 20 5b c3}
condition:
 ( uint16(0) == 0x5a4d and ( 3 of them ) ) or ( all of them )
}
```